République Algérienne Démocratique et Populaire Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A. Mira de Béjaïa

Faculté de Technologies
Département d'Automatique, Télécommunication et d'Électronique (ATE)

Mémoire de Fin d'Etude

En vue de l'obtention du diplôme de Master en télécommunications

Option : Réseaux et Télécommunications

Thème

Conception et mise en place d'un réseau LAN/WAN redondant à haute disponibilité –cas Cevital

Réalisé par :
Mlle. HAROUN Rania
Mlle. KHEMSI Khoukha

Soutenu le 18/ 06/ 2025, Devant le jury composé de :

President	M.BELLAHSENE H.	U.A/Mira Béjaïa
Examinateur	Mme.MEZHOUD N.	U.A/Mira Béjaïa
Encadrant	M.Diboune A.	U.A/Mira Béjaïa

Promotion : 2024/2025

Dédicace

je dédie ce mémoire à mes parents, pour leur amour, leur soutien et les valeurs qu'ils m'ont transmises.

À mes deux frères Mohand et Louay et mes sœurs Yasmine et chanez, pour leur présence constante et leur encouragement tout au long de ce parcours.

À mes amies Djida, Amina, Selma, Tinou, Hanane et ma binome Khoukha et à mes cousines Asma et narimane pour leur amitié précieuse, leur écoute et leurs mots qui m'ont tant portée.

Et à mon mari, pour sa patience, son appui indéfectible et sa foi en moi, même dans les moments les plus difficiles.

Rania

Dédicace

Je dédie ce travail à ma mère Saliha. » Partie très tôt, mais jamais absente de mon cœur. Chaque pas que je fais est guidé par ses douas, son amour éternel et son souvenir qui m'accompagne dans le silence. Puisse Allah t'ouvrir les portes de son vaste paradis. Ce travail, je te l'offre avec toute ma gratitude et ma douleur mêlées.

À mon père Nacer, pour sa force tranquille, ses sacrifices silencieux et son soutien sans faille.

À mon petit frère Yenni. Et à ma sœur Sylia, qui a été toujours présente, complice de chaque étape, soutien fidèle dans les jours durs comme dans les instants de joie.

À mes amies Rania et Djida, merci d'avoir cru en moi même quand j'en doutais moi-même.

khoukha

Remerciements

Un grand merci à Dieu pour nous avoir guidés et inspirés tout au long de ce projet.

Nous tenons à exprimer notre profonde gratitude aux personnes qui ont contribué à son aboutissement et qui nous ont soutenus tout au long de notre parcours.

Tout d'abord, nous tenons à exprimer notre profonde gratitude à notre encadrant, **Mr A.DIBOUNE**, pour la confiance qu'il nous a accordée tout au long de l'élaboration de ce mémoire. Ses conseils avisés, sa rigueur scientifique et son accompagnement constant ont constitué un soutien précieux à chaque étape de notre travail. Sa disponibilité, sa patience et sa capacité à nous orienter avec bienveillance ont grandement contribué à la qualité de ce projet. Grâce à son encadrement attentif et à ses encouragements continus, nous avons pu surmonter les difficultés rencontrées et avancer avec assurance dans notre démarche de recherche. Qu'il trouve ici l'expression de notre sincère reconnaissance et de notre profond respect.

Nous tenons à exprimer notre sincère gratitude envers le groupe **CEVITAL**, et plus particulièrement envers **Mr M.SLIMANI**, pour l'accueil chaleureux qui nous a été réservé et pour l'accompagnement constant dont nous avons bénéficié tout au long de notre stage.

Grâce à leur disponibilité, leur professionnalisme et leur bienveillance, nous avons pu évoluer dans un environnement de travail à la fois stimulant, exigeant et formateur. Cette opportunité nous a permis de mettre en pratique les compétences acquises au cours de notre formation, d'enrichir nos connaissances techniques et d'approfondir notre compréhension du monde professionnel.

Nous leur adressons nos plus vifs remerciements pour cette expérience humaine et professionnelle enrichissante, qui restera une étape marquante de notre parcours.

Nous sommes également reconnaissants envers les membres du jury Madame **MEZHOUD** et Monsieur **BELLAHSENE**, pour l'honneur qu'ils nous font en acceptant d'évaluer notre travail. Nous apprécions leur expertise et leur regard critique, qui nous permettront d'améliorer notre mémoire.

Nous tenons également à remercier tous les enseignants qui nous ont transmis

leur savoir et qui nous ont accompagnés tout au long de notre formation. Leurs cours et leurs conseils ont été essentiels pour notre développement personnel et professionnel. Un grand merci à nos familles et à nos amis pour leur soutien indéfectible, leur encouragement et leur patience tout au long de nos études.

Enfin, nous remercions toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce mémoire. Nous sommes conscients que ce travail n'aurait pas pu être accompli sans votre aide et votre soutien.

Nous vous remercions tous du fond du cœur.

Table des matières

Liste des Figures **ix**

Liste des Tableaux **x**

Introduction Générale **1**

I Problématiques de la haute disponibilité dans les réseaux informatiques **3**

I.1 Introduction 4
I.2 Définition d'un réseau informatique 4
I.3 Les modèles de réseau 4
I.3.1 Le modèle OSI (Open Systems Interconnection) 4
I.3.2 Le modèle TCP/IP (Transmission Control Protocol/Internet Protocol) 5
I.4 La haute disponibilité d'un réseau informatique 7
I.4.1 Définition de la haute disponibilité 7
I.4.2 L'importance de la haute disponibilité 8
I.4.3 Problématiques et solutions 8
I.4.4 Evaluation de risques 9
I.4.4.1 Origines physiques 9
I.4.4.2 Origines humaines 9
I.4.4.3 Origines opérationnelles 9
I.5 Solution 10
I.5.1 Alimentation de secours 10
I.5.1.1 Onduleurs (ups- uninterruptible power supply) . . 10
I.5.1.2 Isolation des circuits électriques 10
I.5.2 Redondance 10
I.5.2.1 Importance de la redondance 10
I.5.2.2 Types de redondance 10
I.5.3 Protocole De Redondance 11
I.5.4 La configuration automatique 11

I.5.4.0.1 Automatisation avec Ansible : 11
I.5.5 audits 12
I.5.5.0.1 Ces audits sont essentiels pour : 12
I.6 Equilibre De Charge 12
I.7 conclusion 13

II Protocoles de redondance réseau 14
II.1 Introduction 15
II.2 Définition de la redondance réseau 15
II.3 Protocoles de redondance niveau équipement 15
II.3.1 HSRP (Hot Standby Router Protocol) 15
II.3.1.1 Fonctionnement de protocole HSRP 16
II.3.1.2 Les différents états d'un routeur HSRP 16
II.3.1.3 Étude de l'entête d'un paquet HSRP 19
II.3.2 VRRP (Virtual Router Redundancy Protocol) 20
II.3.2.1 Fonctionnement de protocole VRRP 20
II.3.2.2 États d'un routeur VRRP 21
II.3.3 GLBP (Gateway Load Blancing Protocol) 21
II.3.3.1 Fonctionnement du GLBP 21
II.3.3.2 Comparaison entre les protocoles FHRP 22
II.3.3.3 Justification du choix du protocole à implémenter . 22
II.4 Protocole de redondance des liasions de commutation 23
II.4.1 Protocole STP (Spaning Tree Protocol) et ses variantes (RSTP, MSTP) 23
II.4.1.1 Fonctionnement du STP 23
II.4.2 Le protocole RSTP 24
II.4.2.1 Etat du port du RSTP 24
II.4.3 MSTP (Multiple Spanning Tree Protocol) 25
II.4.3.1 Fonctionnement du MSTP 25
II.4.3.2 La comparaison des protocoles STP, RSTP, MSTP 25
II.4.4 LACP Link Aggregation Control Protocol) 26
II.4.4.1 Avantages du lacp 27
II.4.5 EtherChannel 27
II.4.5.1 Utilité de l'Ether Channel 27
II.4.5.2 Avantages de l'Etherchannel 28
II.5 protocole de redondance au niveau du réseau étendu WAN 28
II.5.1 BGP (Border Gateway Protocol) : protocole en haute disponibilité 29
II.5.1.1 Type du BGP 29
II.5.1.2 Fonctionnement du BGP 30
II.5.2 OSPF (Open Shortest Path First) 30

II.5.2.1 Fonctionnement d'OSPF 30
II.5.2.2 Avantages d'OSPF 31
II.6 Conclusion 31

III Mise en oeuvre d'une solution de redondance dans un réseau LAN/WAN 32
III.1 Introduction 33
III.2 Présentation de l'entreprise et de son historique 33
III.2.1 Situation géographique de Cevital 33
III.2.2 Valeurs du Groupe CEVITAL 34
III.2.3 Présentation du service informatique 34
III.3 Architecture réseau de Cevital 35
III.3.0.1 Liaisons inter- sites (architecture WAN) 37
III.3.1 Matériels utilisés dans l'architecture réseau : 38
III.3.2 Nombre et modèles des Switchs 40
III.3.3 Nombre et modèles des Serveurs 41
III.3.4 Codification des équipements de Cevital 41
III.3.5 VLANs de l'entreprise 41
III.4 La mise en place d'un réseau LAN redondant 41
III.4.1 Optimisation de la conception 41
III.4.2 Présentation des équipements utilisés 44
III.4.3 Désignation des interfaces 45
III.4.4 VLANs utilisés dans la topologie LAN 45
III.5 Configuration des équipements utilisés 46
III.5.0.1 configuration du base : 46
III.5.0.2 Hostname : 46
III.5.0.3 Configuration de la ligne Console 46
III.5.0.4 Sécurisation du mode privilégié 47
III.5.0.5 Sécurisation des mots de passe 47
III.5.0.6 Configuration d'une bannière : 47
III.5.0.7 Securisation d'accès à distant avec SSH 48
III.5.0.8 Vérification des configurations de base 48
III.5.0.9 Configuration des liaisons Trunk 48
III.5.0.10 Configuration des VLANs : 50
III.5.0.11 Configuration du VTP 50
III.5.0.12 Attribution des ports aux différents VLANs 53
III.5.0.13 Configuration des liens EtherChannel 54
III.5.0.14 Configurations du protocole STP : 55
III.5.0.14.1 La configuration du l'ID du pont 55
III.5.1 Configuration du DHCP : 56
III.5.2 Configuration de protocole HSRP 59

III.5.2.1 Configuration des SVI (Switch Virtual Interface) . 59
III.5.2.2 Configuration de protocole HSRP 61
III.5.2.3 Configurations de Protocole OSPF : 63
III.5.2.4 Test de la haute disponibilité du réseau 65
III.5.2.4.1 Test de haute disponibilité entre Pcs : . . 65
III.5.2.4.2 Test de la haute disponibilité du réseau LAN : 66
III.6 La mise en place d'un réseau WAN redondant 68
III.6.1 Architecture WAN 68
III.6.2 Configuration des équipements du réseau WAN 69
III.6.2.1 VLANs utilisés dans la topologie WAN 69
III.6.2.2 Tableaux des interfaces 70
III.6.2.3 Configuration des interfaces 70
III.6.2.4 Configuration de l'OSPF 71
III.6.2.5 Test de connectivité WAN 73
III.7 Conclusion : 75

Conclusion Générale **76**

Annexes **77**
.1 présentation du simulateur cisco parcket tracer 77
.2 Description générale 77
.3 Ajout d'un équipement 78
.4 Création d'une connexion 79
.5 Configuration d'un équipement 80
.6 Mode simulation 81
.7 Invite de commandes 82

Résumé et Abstract **89**

Table des figures

I.1 **Les couches du modèle OSI** 5
I.2 **La différence entre les couches de modèle OSI - TCP/IP** . 7

II.1 **Diagramme d'état du protocole HSRP** 18
II.2 **Entête d'un paquet HSRP** 20
II.3 **Schéma de principe de fonctionnement du STP** 24
II.4 **Agrégation de liens entre un commutateur et un serveur** . 26
II.5 **Schéma illustre l'interconnexion de deux switch sans Etherchannel** 27
II.6 **Schéma illustre l'interconnexion de deux switch avec Etherchannel** 28
II.7 **BGP Externe** 29
II.8 **BGP interne** 30

III.1 **Logo Cevital** 33
III.2 **Vue satellitaire du complexe CEVITAL** 34
III.3 **Organigramme de la direction système d'information Organigramm** 35
III.4 **Architecture réseau LAN de Cevital** 37
III.5 **Lisaison inter-sites du groupe Cevital** 38
III.6 **Switch distributeur Cisco Catalyst 4507R.** 39
III.7 **Switch Cisco Catalyst 2960** 39
III.8 **Routeur Cisco 2900 .** 39
III.9 **Point d'accès wi-fi Ruckus** 40
III.10 **Pare-feu** 40
III.11 **Data Center** 40
III.12 **Topologie de la nouvelle architecture de réseau LAN de cevital** 44
III.13 **Attribution du nom SWC1 au switch Core** 46
III.14 **Configuration de line console.** 46

III.15Attribution d'un mot de passe pour l'accès au mode privilégiée. 47
III.16curation des mots de pass 47
III.17Configuration d'une bannière motd. 48
III.18Configuration du SSH sur SWC1 48
III.19Configuration du trunk sur SWC2. 48
III.20Configuration du Trunk sur switch d'accès. 49
III.21Vérification des liens trunks sur « SWC1 » 49
III.22Création des VLANs sur SWC1 50
III.23Vérification de la création des VLANs. 50
III.24Configuration de VTP serveur 51
III.25 Vérification de la configuration de VTP serveur. 51
III.26Configuration de VTP client 51
III.27Vérification de la configuration VTP client. 52
III.28Exemple de configuration VTP client sur le Switch accès. 52
III.29Vérification de la configuration VTP client sur le Switch accès 53
III.30 Exemple d'attribution de port au VLAN 2 53
III.31 Vérification de la configuration du mode accès sur le switch SWA1 53
III.32 Vérification si les VLANs ont bien été propagés. 54
III.33Configuration de l'EtherChannel sur SWC1. 54
III.34 Vérification de la configuration d'Etherchannel sur le SWC1 55
III.35 Configuration du STP sur SWC1 55
III.36 Configuration du STP sur SWC2 55
III.37 Vérification du STP sur SWC1 56
III.38 Vérification du STP sur SWC2 56
III.39Instance STP (exemple Vlan 2). 56
III.40Les adresses exclues 125-251 sur SWC1. 57
III.41Les adresses exclues 1-124 sur SWC2. 57
III.42Exemple de création d'un Pool pour le VLAN 2 sur le SWC1 57
III.43Vérification de la création des pools DHCP 58
III.44vérification du DHCP sur le PC0. 59
III.45Configuration d'ip routing. 59
III.46Configuration SVI sur SWC1. 60
III.47Vérification SVI sur SWC1 60
III.48Configuration SVI sur SWC2. 60
III.49Vérification SVI sur SWC2 61
III.50Configuration du HSRP (VLAN 2 à 6). 61

III.51Configuration du HSRP (VLAN 7 à 12). 61
III.52Configuration du HSRP (VLAN 2 à 6). 62
III.53Configuration du HSRP (Vlan 7 à 12). 62
III.54Vérification du HSRP sur SWC1. 62
III.55Vérification du HSRP sur SWC2. 62
III.56Configuration des ports routés sur SWC1. 63
III.57Configuration des ports routés sur SWC2. 63
III.58Configuration des ports routés sur R1. 63
III.59Configuration de l'OSPF sur SWC1. 64
III.60Configuration de l'OSPF sur SWC2. 64
III.61Configuration de l'OSPF sur R1. 64
III.62 Vérification de l'OSPF. 65
III.63Ping continu entre deux PC. 65
III.64Ping continu lors d'une panne de la route principale de VLAN 2 66
III.65 Réactivation de la route principale du VLAN 2 66
III.66Simulation d'une panne sur SWC1 et impact sur la connectivité. 67
III.67 Réactivation du switch principale 68
III.68Architecture WAN de Cevital. 69
III.69Configuration des interfaces du R1 71
III.70Vérification des interfaces de R1 71
III.71Configuration de l'OSPF sur routeur Bejaia. 72
III.72configuration de l'OSPF sur routeur Algerie telecom de bejaia. 72
III.73configuration de l'OSPF sur routeur Algerie Telecom ElKseur 72
III.74configuration de l'OSPF sur routeur Cevital ElKseur . . . 72
III.75Vérification de l'OSPF sur routeur Cevital de Bejaia et routeur Cevital ElKseur. 73
III.76 Vérification de configuration de l'OSPF sur le site distant 73
III.77le ping du pc local au PC distant 73
III.78 verification du ping du pc local au PC distant. 74
III.79 verification du traceroute du route principale. 74
III.80Blokage de la route pricipale 1. 74
III.81 verificationdu ping du route secondaire 2. vers le pc du site distant 75
III.82 verification du traceroute du route secondaire 75
83 environnement de Cisco Packet Tracer. 78
84 Capture d'ajout d'un équipement 79

85 **Capture création d'une connexion entre deux équipements .** 79
86 **Fenêtre de configuration d'un PC.** 80
87 **Fenêtre de configuration d'un PC.** 81
88 **Fenêtre de configuration d'un PC.** 82
89 **Commande prompt.** 83

Liste des tableaux

II.1 **Les différents états d'un routeur HSRP** 17
II.2 **Étude comparative entre HSRP, VRRP, GLBP** 22
II.3 **Comparaison des protocoles Spanning Tree** 26

III.1 **Affectation des VLANs aux directions triées par VLAN** . . 42
III.2 **Les équipements utilisés sur la topologie** 44
III.3 **Désignation des interfaces** 45
III.4 **VLAN pour chaque direction** 45
III.5 **Attribution des adresses IP pour les interfaces des routeurs** 70
III.6 **Attribution des adresses IP pour les interfaces des switchs** 70

Liste des acronymes

LAN	*Local Area Network*
WAN	*Wide Area Network*
IP	*Internet Protocol*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
HTTP	*Hypertext Transfer Protocol*
OSI	*Open Systems Interconnection*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
SMTP	*Simple Mail Transfer Protocol*
ICMP	*Internet Control Message Protocol*
ATM	*Asynchronous Transfer Protocol*
ARP	*Address Resolution Protocol*
MAC	*Media Access Control*
DHCP	*Dynamic Host Configuration Protocol*
VLAN	*Virtuel Local Area Network*
DSI	*Direction du Systeme d'information*
FHRP	*First Hop Redundancy Protocol*
HSRP	*Hot Standby Router Protocoll*
VRRP	*Virtuel Router Redundancy Protocol*

GLBP *Gateway Load Balancing Protocol*

STP *Spanning Three Protocoll*

RSTP *Rapid Spanning Three Protocol*

MSTP *Multi Spanning Three Protocol*

BGP *Bordre Gateway Protocol*

VTP *Vlan turking Protocol*

LACP *Link Aggregation Control Protocol*

EIGRP *Enchanced Interior Gateway Routing Protocol*

OSPF *Open Shortest Patch First*

DMZ *Zone démilitarisée*

SSH *Secure Socket Shell*

SVI *Switch Vituel Interface*

FH *Faisceaux Hertiziens*

WIFI *Wireless Fidelity*

Introduction Générale

Dans un monde de plus en plus connecté, les réseaux de télécommunications et informatiques jouent un rôle essentiel au sein des entreprises et des organisations. Ces réseaux, qui servent de base à la communication et à l'échange d'informations, doivent être conçus et gérés de manière efficace pour répondre aux exigences croissantes en termes de performance et de disponibilité.

Cependant, la disponibilité des réseaux peut être fortement perturbée par des pannes techniques, des attaques informatiques, des catastrophes naturelles ou d'autres risques. Les interruptions du réseau peuvent avoir de graves conséquences pour l'entreprise, comme des pertes financières et des blocages dans les activités quotidiennes.

Pour répondre à cette problématique, les réseaux redondants et à haute disponibilité sont de plus en plus déployés afin d'assurer la continuité opérationnelle de l'entreprise. Ils intègrent des liens de secours, des mécanismes de basculement automatique et d'autres fonctionnalités de résilience permettant de minimiser les interruptions en cas de défaillance.

Ce projet de fin d'études s'atricule autour de la mise en place d'un réseau LAN/WAN redondant, destiné à garantir la continuité du réseau et à réduire les interruptions en cas de pannes matérielles. Il s'agit de concevoir une solution de réseau redondant adaptée à ces besoins, puis de la déployer sur les équipements en configurant les protocoles de routage dynamique, les liens de secours, et les autres mécanismes de redondance. Cette étude se base sur le cas concret de Cevital Agro-industrie, une entreprise importante active dans plusieurs secteurs en Algérie.

Le présent mémoire comporte trois chapitres :

Le premier chapitre pose les bases théoriques en abordant les principes fondamentaux des réseaux informatiques : les architectures réseau, les différents types de réseaux, les modèles OSI et TCP/IP , la haute disponibilité, ainsi qu'une présentation des différentes solutions permettant de l'assurer.

Au cours du deuxième chapitre, nous abordons la problématique de la haute disponibilité ainsi que son fonctionnement, en expliquant comment le garantir efficacement dans un réseau LAN/WAN d'entreprise. Nous présentons également les différents protocoles et mécanismes qui permettent d'assurer la continuité et la ré-

silience des services en cas de défaillance, tels que HSRP,VRRP,GLBP,STP,MSTP,OSPF, RSTP, BPDU et Etherchannel.

Le troisième chapitre est divisé en deux parties. Dans la première, nous présentons la conception du modèle LAN, en détaillant les étapes de préparation, la création du schéma réseau, la nomination des équipements, la configuration des interfaces ainsi que la mise en place des VLAN. Cette partie se termine par la réalisation de ce modèle à l'aide du simulateur Packet Tracer. Dans la seconde partie, nous procédons à l'interconnexion du modèle WAN avec les autres sites distants de l'entreprise afin de configurer un réseau WAN optimisé. Enfin, des tests de validation sont effectués pour vérifier si les objectifs fixés ont été atteints.

Chapitre I

Problématiques de la haute disponibilité dans les réseaux informatiques

I.1 Introduction

Afin de mener à bien notre étude sur l'optimisation d'un réseau local étendu, ce chapitre présentera les concepts théoriques fondamentaux relatifs aux réseaux informatiques. Nous y aborderons également une étude détaillée de la haute disponibilité, ainsi qu'une présentation des différentes solutions permettant de l'assurer.

I.2 Définition d'un réseau informatique

Un réseau informatique, également appelé data communication network (DCN) en anglais, correspond à un ensemble de moyens matériels et logiciels reliés entre eux leur permettant d'échanger des informations et de partager des ressources. La liaison entre les différents éléments est faite avec ou sans fil [1].

La mise en place d'un réseau nécessite une certaine expertise technique, notamment en ce qui concerne la sécurité, la configuration des paramètres réseau et la résolution des problèmes. Il existe également des normes et des protocoles de communication standardisés qui facilitent l'interopérabilité des dispositifs sur un réseau [2] .

I.3 Les modèles de réseau

Les modèles réseau sont des modèles conceptuels qui définissent la structure, les fonctions et les interactions des différent s couches du réseau informatique. Les modèles de réseau les plus couramment utilisés sont le modèle OSI et TCP/IP [3].

I.3.1 Le modèle OSI (Open Systems Interconnection)

Le modèle OSI (Open Systems Interconnection) est une norme de communication de tous les systèmes informatiques en réseaux. C'est un modèle de communications entre ordinateurs proposé par l'ISO (Organisation internationale de normalisation) qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions. Le modèle comporte sept couches succinctement présentées ci-dessus de bas en haut et détaillées dans leurs articles respectifs [4].

	PDU	Couche		Fonction
Couches hautes	Donnée	7	Application	Point d'accès aux services réseau
		6	Présentation	Gère le chiffrement et le déchiffrement des données, convertit les données machine en données exploitables par n'importe quelle autre machine
		5	Session	Communication Interhost, gère les sessions entre les différentes applications
	Segment / Datagramme	4	Transport	Connexion de bout en bout, connectabilité et contrôle de flux ; notion de port (TCP et UDP)
Couches matérielles	Paquet	3	Réseau	Détermine le parcours des données et l'adressage logique (adresse IP)
	Trame	2	Liaison	Adressage physique (adresse MAC)
	Bit / Symbole	1	Physique	Transmission des signaux sous forme numérique ou analogique

FIGURE I.1 – **Les couches du modèle OSI**
[3]

I.3.2 Le modèle TCP/IP (Transmission Control Protocol/Internet Protocol)

Le modèle TCP/IP est plus simple qu'OSI, avec seulement quatre couches Accès réseau, Internet, transport et application. La différence avec OSI est simplement que certaines couches ont été fusionnées. La couche d'accès réseau de TCP/IP regroupe notamment les couches physiques et liaison d'OSI. De même, la couche application de TCP/IP regroupe les couches session, application et présentation d'OSI [5] .

— Voici les quatre couches du modèle TCP/IP [6] :

— **La couche d'accés réseau :** Elle regroupe deux couches du modèle OSI : la couche physique et la couche liaison de données.

  — La couche physique : Elle assure l'émission et la réception des données sous forme de signaux adaptés aux supports utilisés (électriques, lumineux, radio). Elle définit les normes des supports de transmission (câbles en cuivre, fibres optiques, radio), ainsi que les caractéristiques techniques comme les connecteurs, le codage, la synchronisation et la distance maximale autorisée.

  — la couche liaison de données : Elle organise et sécurise le transfert des informations. Elle regroupe les bits issus de la couche physique pour former des trames bien délimitées, grâce à des séquences particulières de bits qui marquent le début et la fin de chaque trame. Elle attribue à chaque équipement une adresse physique appelée adresse MAC. Cette couche contrôle également l'accès au support de transmission pour éviter les collisions, en utilisant des protocoles comme CSMA/CD ou CSMA/CA. Enfin, elle intègre des mécanismes de détection d'erreurs, comme le contrôle par CRC, pour garantir l'intégrité des données transmises.

— **La couche internet :** Elle assure l'acheminement des données sur le réseau en réalisant l'adressage logique des équipements (IPv4, IPv6) et le routage des paquets à travers différents réseaux (protocoles RIP, OSPF, EIGRP, BGP). Elle gère aussi la fragmentation et le réassemblage des paquets trop volumineux, détecte les paquets perdus ou corrompus, et contribue à la gestion du trafic pour éviter la congestion du réseau..

— **La couche transport :** Elle est chargée d'assurer la transmission fiable des données entre les applications. Elle segmente les données à l'envoi et les réassemble à la réception. Grâce au protocole TCP, elle détecte les erreurs, retransmet les segments perdus et ajuste le flux de données pour éviter la surcharge réseau (grâce au mécanisme de fenêtre glissante).

Elle permet aussi le multiplexage : plusieurs applications peuvent utiliser simultanément le réseau grâce à des ports. Enfin, elle établit des connexions fiables via un processus d'initialisation en trois étapes appelé handshake (SYN, SYN-ACK, ACK) [7].

— **La couche application :** Cette couche fournit des services de réseau aux applications utilisateur, tels que la messagerie électronique, la navigation sur le Web et le transfert de fichiers . Les protocoles courants à cette couche incluent HTTP, FTP, SMTP et DNS .

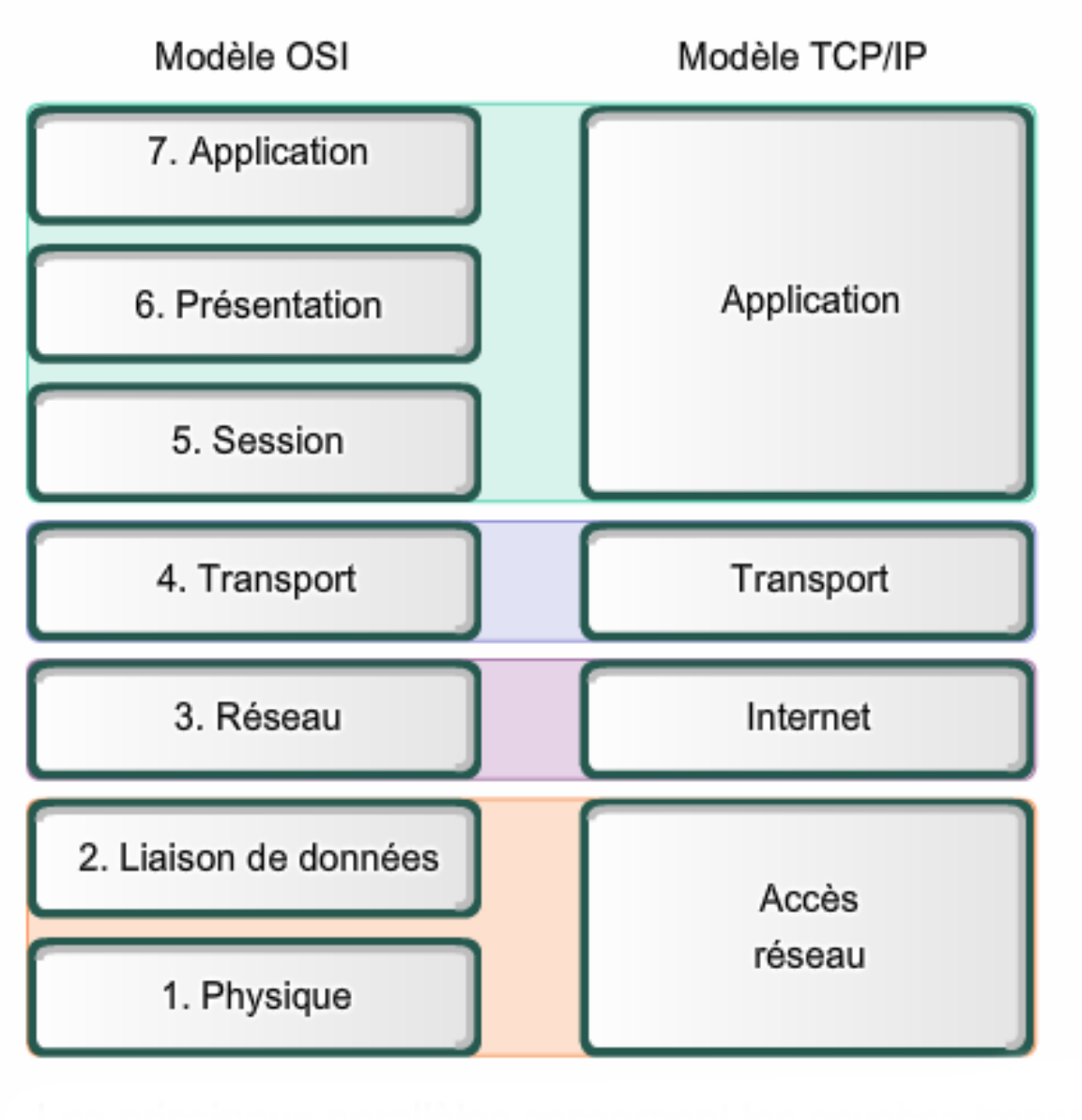

FIGURE I.2 – **La différence entre les couches de modèle OSI - TCP/IP** [8]

I.4 La haute disponibilité d'un réseau informatique

I.4.1 Définition de la haute disponibilité

La haute disponibilité (ou High Availability ou HA) fait référence à la capacité d'un système, d'une application ou d'un service informatique à rester opérationnel et accessible pour les utilisateurs, même en présence de pannes, d'incidents ou de défaillances. L'objectif principal de la haute disponibilité est d'assurer la continuité des opérations et de minimiser les interruptions ou les temps d'arrêt [9].

Elle permet d'assurer et de garantir le bon fonctionnement des services ou applications proposées et ce 7j/7 et 24h/24. Cela consiste donc à mettre en place

toutes les actions et dispositions techniques pour qu'une infrastructure informatique soit toujours disponible en appliquant certains principes tels que la réplication des données, la sauvegarde, la répartition de la charge, la redondance, etc. pour limiter l'indisponibilité d'un SI . Dans le prochain chapitre, nous présenterons quelques notions et plusieurs définitions relatives à la conception des systèmes de reconnaissance d'emotion[10].

I.4.2 L'importance de la haute disponibilité

La haute disponibilité est essentielle dans de nombreux domaines, tels que les services bancaires en ligne, les sites de commerce électronique, les systèmes de réservation, les centres de données, les réseaux informatiques et les infrastructures critiques. Voici quelques-unes des raisons pour lesquelles la haute disponibilité est importante [9].

- **Continuité des opérations :** La haute disponibilité garantit que les services et les systèmes restent opérationnels même en cas de pannes matérielles, de pannes de logiciels, de cyberattaques ou d'autres problèmes techniques. Cela permet aux entreprises de maintenir leurs activités sans interruptions majeures, ce qui est crucial pour la productivité et la satisfaction des clients .
- **Réduction des temps d'arrêt :** En ayant des systèmes hautement disponibles, les temps d'arrêt sont réduits au minimum. Cela permet de limiter les pertes financières, la perte de productivité et les impacts négatifs sur la réputation de l'entreprise.
- **Évolutivité :** La haute disponibilité facilite l'évolutivité des systèmes et des applications. Elle permet d'ajouter de nouvelles ressources, de répartir la charge sur plusieurs serveurs et de gérer efficacement les pics de trafic sans compromettre la disponibilité.

I.4.3 Problématiques et solutions

Une infrastructure à haute disponibilité doit détecter et éliminer les points de défaillance uniques qui pourraient augmenter les temps d'arrêt système et empêcher les entreprises d'atteindre leurs objectifs de performances. Un point de défaillance unique désigne un aspect de l'infrastructure capable de déconnecter l'ensemble du système en cas de panne. Dans les systèmes complexes, il peut y en avoir plusieurs.

En outre, les entreprises doivent prendre en compte les différents types de défaillances qui menacent les infrastructures informatiques modernes et complexes. Il peut s'agir de pannes du matériel, des logiciels (à la fois au niveau du système

d'exploitation et des applications en cours d'exécution) ou des services (comme l'indisponibilité du réseau, les latences et la dégradation des services cloud ou des performances), ou encore de défaillances externes comme une panne de courant [6].

I.4.4 Evaluation de risques

La panne d'un système informatique peut causer une perte de productivité et d'argent, voire des pertes matérielles ou humaines dans certains cas critiques. Il est ainsi essentiel d'évaluer les risques liés à un dysfonctionnement d'une des composantes du système d'information et de prévoir des moyens et mesures permettant d'éviter ou de rétablir dans des temps acceptables tout incident. Comme chacun le sait, les risques de pannes d'un système informatique en réseau sont nombreux. L'origine des fautes peut être schématisée de la manière suivante[11] :

I.4.4.1 Origines physiques

Elles peuvent être d'origine naturelle ou humaine :

— Désastre naturel (inondation, séisme, incendie).

— Environnement (intempéries, taux d'humanité de l'air , température).

— Panne matérielle.

— Panne de réseau.

— Coupure électrique.

I.4.4.2 Origines humaines

Elles peuvent être soit intentionnelles soit fortuites :

— Erreur de conception (bogue logiciel, mauvais dimensionnement du réseau).

— Porte dérobée.

— Sabotage.

— Piratage.

I.4.4.3 Origines opérationnelles

Elles sont liées à un état du système à un moment donné :

— Bogue logiciel.

— Dysfonctionnement logicil.

I.5 Solution

I.5.1 Alimentation de secours

Dans un réseau Lan Wan, l'alimentation de secours est essentielle pour garantir la haute disponibilité et éviter les interruptions de service en cas de coupure de courant

I.5.1.1 Onduleurs (ups- uninterruptible power supply)

Il sert à protéger les appareils électroniques contre les dommages immédiats pouvant être causés par des irrégularités électriques, et il contribue à prévenir les pertes de données ou les interruptions de tâches [12].

I.5.1.2 Isolation des circuits électriques

Une autre solution serait de distribuer l'énergie sur plusieurs circuits séparés pour prévenir une coupure totale d'alimentation en cas de surcharge ou de court-circuit[13].

I.5.2 Redondance

La redondance nécessite l'existence de composants multiples pour assurer leur disponibilité en cas de panne d'un élément

I.5.2.1 Importance de la redondance

L'un des principaux avantages de la redondance est d'améliorer la fiabilité du réseau face aux défaillances Elle permet de garantir un fonctionnement continu, même en cas de panne matérielle ou logicielle, en identifiant rapidement les fautes et enivant des mécanismes de récupération automatique. Grâce à ces solutions, le réseau peut se rétablir sans intervention humaine, assurant ainsi une haute disponibilité du service. Cette approche repose notamment sur la duplication des composants et le basculement automatique vers des éléments de secours en cas de défaillance[14].

I.5.2.2 Types de redondance

— **La redondance matérielle :** Cela signifie l'intégration d'un appareil ou d'un composant en double dans le réseau. Ce processus est mis en œuvre en cas de panne d'un périphérique ou d'un élément clé, avec pour objectif de minimiser le temps d'interruption[15].

— **La redondance réseau :** Cela implique la duplication des chemins réseau afin de garantir une accessibilité permanente en cas de défaillance. Cela signifie qu'il existe des équipements ou des connexions de secours permettant un accès immédiat en cas de panne d'un élément du réseau, en utilisant des protocoles comme STP, HSRP et VRRP[16].

I.5.3 Protocole De Redondance

Diverses technologies et protocoles contribuent à la mise en place d'une infrastructure hautement disponible :

— **Le protocole Etherchannel** EtherChannel est une technologie de liaison de ports qui permet de regrouper plusieurs liaisons physiques en une seule liaison logique pour obtenir un lien virtuel de meilleure capacité[17].

— **Le protocole STP (Spanning-Tree Protocole)** L'algorithme STP permet de créer une topologie logique sans boucle en désactivant les liens redondants et en ne laissant qu'un seul chemin actif entre les noeuds du réseau. Il utilise des messages BPDU (Bridge Protocol Data Unit) pour échanger des informations entre les commutateurs et détecter les boucles[18].

— **Le protocole HSRP (Hot standby Router Protocol)** Le protocole HSRP est un protocole de redondance propriétaire de Cisco qui permet d'établir une passerelle par défaut tolérante aux pannes. Il peut être mis en place sur un routeur ou un switch de niveau 3 du modèle OSI. Il est un bon choix pour les réseaux Cisco qui n'ont pas besoin d'équilibrage de charge[19].

— **Le protocole VRRP (Virtuel Router Redundancy Protocol)** VRRP spécifique un protocole d'élection qui assigne dynamiquement les responsabilités pour un routeur virtuel à un concentrateur VPN provenant d'un réseau LAN. Le routeur VRRP, qui contrôle les adresses IP associées au routeur virtuel, est appelé Maître, et les transferts de paquets sont redirigés vers ses adresses IP[20].

I.5.4 La configuration automatique

L'avantage de l'automatisation est que grâce à son caractère idempotent, agentless, et extensible, elle permet un plus grand passage à l'échelle et par conséquent une duplication facile des infrastructures

— **Exemple**

I.5.4.0.1 Automatisation avec Ansible : Ansible est un environnement d'automatisation open-source permettant l'automatisation et la gestion des périphérique réseaux notamment les serveurs, le déploiement d'applications et la configuration

des infrastructures. Ansible est agentless i.e. aucun logiciel agent n'est nécessaire à installer sur les machines cibles. De plus, il permet d'utilise SSH pour exécuter les commandes à distance[21].

I.5.5 audits

Un audit de sécurité est une évaluation systématique et méthodique des mesures de sécurité mises en place dans un système informatique, un réseau ou une organisation. Il vise à identifier les vulnérabilités, les risques potentiels et les failles de sécurité afin de proposer des recommandations pour renforcer la protection des données et des infrastructures contre les menaces externes et internes[22].

I.5.5.0.1 Ces audits sont essentiels pour :

- assurer la conformité réglementaire RGPD (règlement général sur la protection des données).
- prévenir les attaques informatiques
- maintenir la confidentialité, l'intégrité et la disponibilité des informations sensible
- protection des dondonnées sensibles DoS (Denial of Service)[22].

I.6 Equilibre De Charge

L'équilibrage de charge est un élément important lors de la mise en place de services amenés à croître. Il faut s'assurer que la capacité à monter en charge soit la plus optimale possible afin d'éviter toute dégradation que ce soit en terme de performances ou de fiabilité lors d'affluences importantes. Le principe de base de l'équilibrage de charge (Load Balancing) consiste à effectuer une distribution des tâches à des machines de façon intelligente.[23] Ses principaux objectifs sont :

- Amélioration des temps de réponse des services.
- capacité à pallier la défaillance d'une ou de plusieurs machines.
- Ajoute de nouveaux serveurs sans interruption de service ,il est inhérent au processus de transfert dans le routeur et est automatiquement activé si la table de routage a plusieurs chemins vers une destination.

Il est basé sur des protocoles de routage standard, tels que

- Enhanced Interior Gateway Routing Protocol (EIGRP).
- Protocole OSPF (Open Shortest Path First).
- Interior Gateway Routing Protocol (IGRP). Grâce à ces protocoles, les réseaux peuvent répartir efficacement le trafic, éviter les engorgements et garantir une meilleure résilience face aux pannes.

I.7 conclusion

Dans ce chapitre, nous avons examiné les concepts fondamentaux des réseaux informatiques, en mettant l'accent sur l'importance de la haute disponibilité et mentionner des stratégies clés telles que la redondance, l'équilibre de charge. Ces éléments sont essentiels pour assurer un accès continue aux services.

Chapitre II

Protocoles de redondance réseau

II.1 Introduction

Après avoir abordé la notion de haute disponibilité dans le chapitre précédent, nous allons définir plus en détail ce concept dans ce chapitre, en étudiant son fonctionnement, en expliquant comment le garantir efficacement dans un réseau LAN/WAN d'entreprise. Pour cela, nous présenterons les différents protocoles et mécanismes qui permettent d'assurer la continuité et la résilience des services en cas de défaillance.

II.2 Définition de la redondance réseau

La redondance réseau est un processus qui consiste à ajouter des périphériques réseau et des lignes de communication suplémentaires pour maintenir la connectivité si la voie principale, un segment ou un lien est en panne [24].

Elle est d'une importance capitale pour les entreprises dans la garantie de la disponibilité, de la fiabilité et de la résilience des communications et des opérations informatiques [25].

Les protocoles de redondances peuvent être subdivisés en trois classes :

1. Protocoles de redondance niveau équipement
2. Protocole de redondance niveau liaison de commutation
3. Protocoles de redondance niveau réseau étendu

Nous détaillerons les foctionalités de chacune de ces classes dans les trois séctions qui suivent.

II.3 Protocoles de redondance niveau équipement

Dans les environnements réseau, la disponibilité et la fiabilité des services sont essentielles pour garantir un fonctionnement ininterrompu. Les protocoles de redondance de passerelle jouent un rôle crucial en fournissant des mécanismes permettant la continuité du service en cas de panne de périphérique réseau. Trois des protocoles les plus utilisés pour assurer cette redondance sont HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol) et GLBP (Gateway Load Balancing Protocol) [26].

II.3.1 HSRP (Hot Standby Router Protocol)

HSRP est un protocole de redondance du premier saut (FHRP, First Hop redundancy Protocols), propriétaire Cisco. Il permet ainsi à plusieurs routeurs de travailler ensemble pour former un routeur virtuel unique, assurant une continuité de service en cas de défaillance d'un routeur physique. Il offre plusieurs avantages,

notamment la haute disponibilité, la redondance et la flexibilité, mais peut également présenter des limitations, telles que la dépendance à la priorité[19].

II.3.1.1 Fonctionnement de protocole HSRP

HSPR repose sur plusieurs points essentiels nous eprésentons ci-dessous :

— Le HSRP permet à plusieurs routeurs de former un groupe HSRP, où un routeur est désigné comme routeur actif (active router) et les autres comme routeurs de secours (standby routers).

— Chaque routeur HSRP se voit attribuer une priorité, exprimée par une valeur comprise entre 1 et 255.

— Le routeur avec la plus haute priorité devient le routeur actif. En cas d'égalité de priorité, le routeur avec l'adresse IP la plus élevée devient le routeur actif.

— Tous les routeurs du groupe HSRP partagent une adresse IP virtuelle et une adresse MAC virtuelle, qui servent de passerelle par défaut pour les hôtes du réseau local.

— Le routeur actif est responsable de la transmission du trafic réseau, tandis que les routeurs de secours restent en veille et surveillent l'état du routeur actif.

— Les routeurs HSRP communiquent entre eux en envoyant des messages de type "Hello" en multicast à l'adresse 224.0.0.2 (pour version 1) ,224.0.0.102 (pour version 2) pour se tenir mutuellement informés de leurs priorités et de leurs états (actif ou de secours).

— Si le routeur actif devient inaccessible, l'un des routeurs de secours prend automatiquement le relais et devient le nouveau routeur actif, assurant ainsi une continuité de service.

— Le temps nécessaire pour qu'un routeur de secours prenne le relais en cas de défaillance du routeur actif, est généralement est égale à 10 secondes (Le Hold Timer est de 10 secondes, soit 3 * le Hello Timer + 1 seconde) [27].

II.3.1.2 Les différents états d'un routeur HSRP

Après la configuration de HSRP, chaque routeur HSRP passera par plusieurs états avant de devenir un routeur actif ou de secours , cet état (champ "state") est codé sur un octet dans le paquet HSRP. Table II.1 résume ses différentes états et valeurs :

Valeur de l'octet	État	Description
0	Initial	C'est l'état au démarrage du routeur. Il indique que le HSRP n'est pas actif. Cet état est présent lorsqu'un changement de configuration opère ou quand une interface devient opérationnelle pour la première fois.
1	Learn	Indique que le routeur ne connaît pas encore l'IP du routeur virtuel du groupe HSRP et n'a pas encore vu de messages «Hello» d'un autre routeur actif du groupe HSRP. Il attend alors et reste à l'écoute d'un message du routeur actif.
2	Listen	Indique que le routeur connaît l'IP du routeur virtuel du groupe HSRP mais ne connaît pas le routeur actif ou le routeur passif. Il attend et reste à l'écoute de messages «Hello» de ces routeurs.
4	Speak	Indique que le routeur envoie des paquets «Hello» et participe à l'élection du routeur actif (active) et du routeur passif (standby). Un routeur ne peut passer en «Speak» que s'il connaît déjà l'adresse du routeur virtuel (qu'il est déjà passé en «Listen»).
8	Standby	Indique que le routeur est prêt à prendre le relais en cas de perte du routeur actif. Il envoie de manière périodique des messages «Hello».
16	Active	C'est le routeur qui fait suivre les paquets qui sont envoyés au routeur virtuel du groupe HSRP par les hôtes du réseau. Il envoie périodiquement des messages «Hello» en multicast sur le port 1985 pour indiquer son état.

TABLE II.1 – **Les différents états d'un routeur HSRP**
[27]

A illustrer par une automate de transition d'état, voir la figure ci-dessous

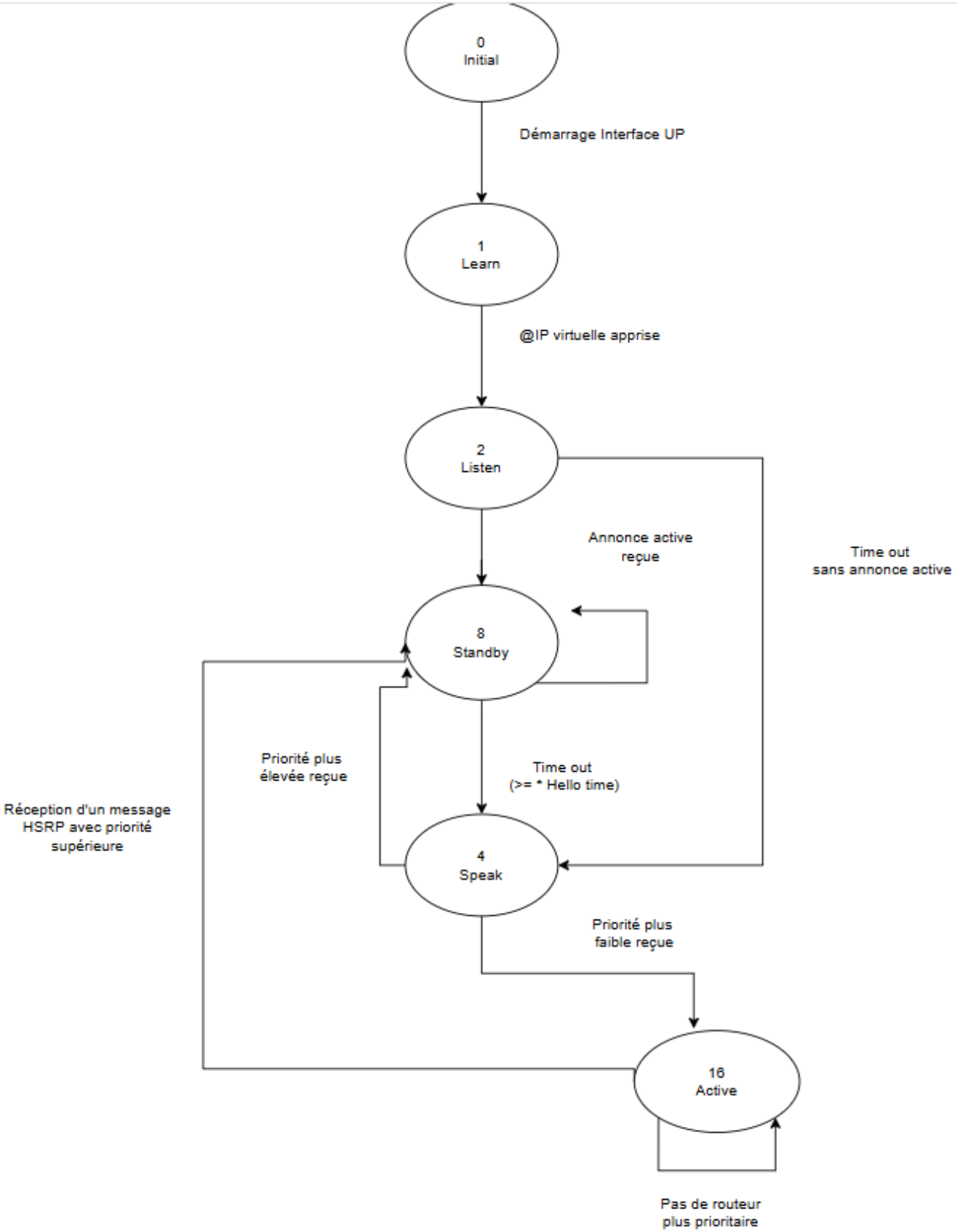

FIGURE II.1 – **Diagramme d'état du protocole HSRP**

II.3.1.3 Étude de l'entête d'un paquet HSRP

L'analyse de la composition de l'en-tête d'un paquet HSRP est essentielle pour comprendre le fonctionnement du protocole HSRP. L'en-tête d'un paquet HSRP contient plusieurs champs importants :

- **Version :** Indique la version du protocole HSRP utilisée ; ce champ occupe 1 octet dans l'en-tête.
- **Op Code :** Indique le type de message transmis par le paquet, Ce champ occupe 1 octet. Trois types de messages distincts existent, chacun ayant une valeur et une signification propres :
  - **0 - Hello :** Ce message est émis périodiquement par les routeurs Actif et Standby afin de maintenir la communication et de signaler leur présence au sein du groupe HSRP.
  - **1 - Coup :** Ce message est envoyé par un routeur Standby qui souhaite prendre la relève en tant que routeur Actif. Il peut être déclenché par la détection d'une défaillance du routeur Actif ou par une décision manuelle de l'administrateur.
  - **2 – Resign :** Ce message est transmis par un routeur Actif qui souhaite se décharger de ses responsabilités et céder la place à un autre routeur Standby.
- **State :** Indique l'état du routeur, il occupe 1 octet dans l'en-tête .
- **Hellotime :** Détermine l'intervalle de temps entre les messages Hello envoyés par les routeurs Actif et Standby, il occupe 1 octets dans l'entête.
- **Holdtime :** Définit le délai maximal après lequel un routeur est considéré comme inactif s'il n'a pas reçu de message Hello. Il doit être au moins trois fois supérieur à la valeur de Hellotime pour garantir une détection fiable des défaillances, il occupe 1 octets dans l'entête.
- **Priority :** Indique la priorité du routeur dans le groupe HSRP, occupe 1 octet dans l'entête.
- **Group :** Indique le numéro du Standby Group, il permet de différencier plusieurs groupes HSRP coexistant sur le même réseau, occupe 1 octet dans l'entête.
- **Authentication Data :** Contient des informations d'authentification pour garantir la sécurité du protocole HSRP, occupe 8 octet dans l'entête.
- **Virtual IP Address :** Désigne l'adresse IP virtuelle attribuée au groupe HSRP.Cette adresse IP est utilisée par les clients pour accéder aux services du groupe, quelle que soit le routeur actif. Ce champ occupe 4 octet dans l'entête [27].

.

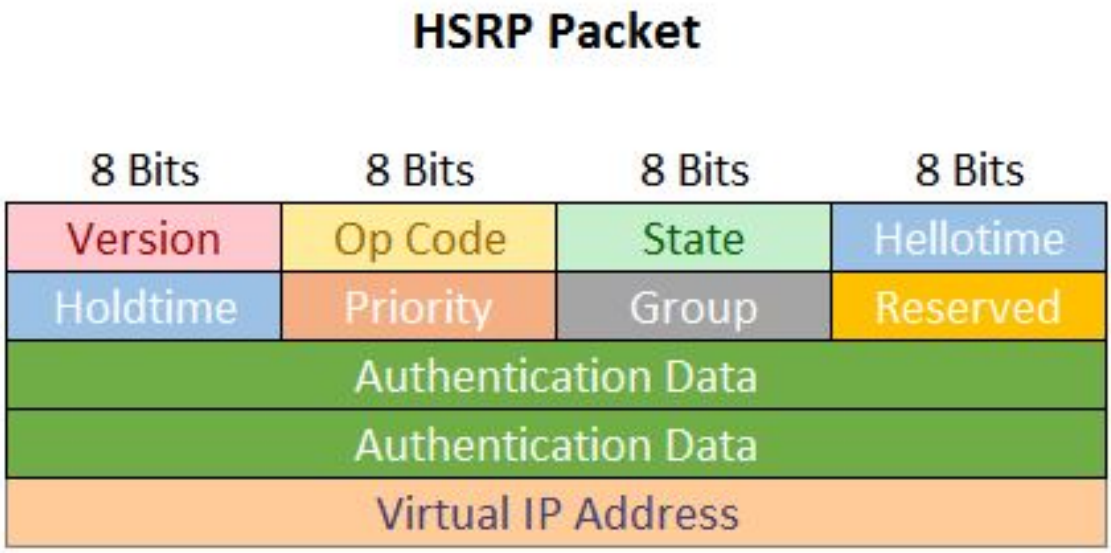

FIGURE II.2 – **Entête d'un paquet HSRP**
[28]

II.3.2 VRRP (Virtual Router Redundancy Protocol)

VRRP est un protocole de redondance de routeur conçu pour fournir une haute disponibilité et une fiabilité dans les réseaux IP. Comme HSRP, VRRP permet à plusieurs routeurs de fonctionner ensemble au sein d'un groupe pour former une passerelle virtuelle. Cependant, VRRP est une norme définie par L'IETF (Internet Engineering Task Force), ce qui signifie qu'elle ne se limite pas aux équipements Cisco et qu'elle est interopérable entre différents fabricants d'équipements réseau [20].

II.3.2.1 Fonctionnement de protocole VRRP

Le processus de fonctionnement de VRRP peut être résumé en plusieurs étapes clés [20] :

1. Adresse IP virtuelle partagée

— Une IP virtuelle (VIP) est partagée entre tous les routeurs d'un groupe VRRP.

— Cette IP est configurée comme passerelle par défaut sur les hôtes du réseau.

2. Élection du Master

— Chaque routeur est configuré avec une priorité dont la valeur est comprise entre 0 et 255.

— Le routeur ayant la plus haute priorité devient le Master et détient l'adresse IP virtuelle.

— Les autres sont en état Backup.

3. Publications VRRP

— Le Master envoie régulièrement des annonces VRRP, à un intervalle d'une seconde par défaut.

— Ces annonces indiquent aux routeurs Backup que le Master est toujours actif.

4. Surveillance et bascule

— Si les routeurs Backup ne reçoivent plus d'annonces dans un certain délai (généralement 3 fois l'intervalle d'annonce), ils supposent que le Master est en panne.

— Un nouveau Master est élu parmi les Backups (le plus prioritaire).

— Ce nouveau Master prend l'IP virtuelle et commence à envoyer les annonces.

5. Préemption (optionnelle)

— Si l'ancien Master revient et qu'il a une priorité plus élevée, il peut reprendre automatiquement son rôle.

— Cela dépend du paramètre "preempt", qui peut être activé ou désactivé.

II.3.2.2 États d'un routeur VRRP

— **Init :** état initial à la mise en service.

— **Backup :** surveille le Master, prêt à basculer.

— **Master :** détient l'adresse IP virtuelle, envoie les annonces[20].

II.3.3 GLBP (Gateway Load Blancing Protocol)

GLBP est un autre protocole de redondance de routeur développé par Cisco. Contrairement à HSRP et VRRP, GLBP va au-delà de la simple redondance en répartissant la charge de trafic sur plusieurs routeurs actifs. Ce protocole est conçu pour optimiser l'utilisation des ressources réseaux et améliorer les performances en équilibrant efficacement la charge [29].

II.3.3.1 Fonctionnement du GLBP

Le GLBP fonctionne en élisant un routeur AVG (Active Virtual Gateway) parmi les routeurs participant au groupe GLBP. L'AVG est responsable de l'attribution de l'adresse IP virtuelle à un ou plusieurs routeurs dits AVF (Active Virtual Forwarders). Les AVF sont responsables de la transmission des paquets vers les machines du réseau. Le fonctionement du protocole GBLP peut être résumé en trois étapes [29] :

— **1. Election de l'AVG :** Le routeur avec la plus haute priorité est élu comme AVG. Ce routeur est responsable de l'allocation de l'adresse IP virtuelle et de la gestion des AVF .
— **2. Répartition des AVF :** L'AVG distribue les paquets réseau entre les AVF disponibles, ce qui permet d'équilibrer la charge.
— **3. Équilibrage de charge :** L'AVG envoie les réponses ARP (Address Resolution Protocol) avec des adresses MAC différentes, chacune correspondant à un AVF différent, ce qui répartit la charge de manière transparente entre les routeurs [29].

Le GLBP permet d'utiliser toutes les passerelles disponibles, améliorant ainsi l'efficacité du réseau. Si un AVF tombe en panne, un autre routeur prend immédiatement le relais, assurant ainsi la continuité du service.

II.3.3.2 Comparaison entre les protocoles FHRP

Tableau II.2 résume une étude comparatives entre les protocoles de redondance niveau equipement décrits dans les sections precedentes.

Critère	**HSRP**	**VRRP**	**GLBP**
Développeur du protocole	Cisco	Standard	Cisco
Normalisation	Propriétaire	Ouvert (RFC 5798)	Propriétaire
Nombre de routeurs actifs	1 actif (les autres en veille)	1 actif (Master)	Plusieurs actifs (Jusqu'à 4)
Équilibrage de charge	Non	Non	Oui
Priorité par défaut	100	100	100
Méthode d'élection	Priorité + IP haute	Priorité + IP haute	Priorité + IP haute + pondération
Temps de convergence	10 sec (réductible)	3 sec (rapide)	1 à 10 sec
Support IPv6	Oui	Oui (VRRPv3)	Oui
Cas d'utilisation	Réseaux Cisco simples	Réseaux mixtes	réseau Cisco avancé
Complexité	Simple	Moyenne	Complexe

TABLE II.2 – **Étude comparative entre HSRP, VRRP, GLBP** [30]

II.3.3.3 Justification du choix du protocole à implémenter

Nous avons choisi d'implémenter le protocole HSRP pour assurer la haute disponibilité du réseau. Il permet à plusieurs routeurs de se partager une adresse IP virtuelle, garantissant la continuité de service en cas de panne.

L'infrastrure réseau de l'entreprise est basée sur du matériel CISCO , Ainsi HSRP permet une meilleur integration et un meilleur support des fonctionalités avancés comme interface tracking (permet au routeur actif ou standby de surveiller une ou plusieurs interfaces locales).

II.4 Protocole de redondance des liasions de commutation

L'IEEE a développé trois protocoles : le protocole STP (Spanning Tree Protocol), puis le RSTP (Rapid Spanning Tree Protocol) et enfin le MSTP (Multiple Spanning Tree Protocol). Tous trois servent à éliminer les boucles réseau . Les périphériques exécutant STP, RSTP ou MSTP échangent des BPDU pour calculer le l'arbre couvrant [18].

II.4.1 Protocole STP (Spaning Tree Protocol) et ses variantes (RSTP, MSTP)

Le Spanning Tree Protocol (STP) est un protocole de couche 2 du modèle OSI utilisé dans les réseaux Ethernet pour empêcher la formation de boucles de commutation lorsque plusieurs chemins existent entre les commutateurs. Son objectif est l'élimination des boucles de commutation et l'évitement des tempêtes de diffusion, en désactivant automatiquement certains liens redondants. Cela permet de maintenir un réseau stable, tout en gardant la possibilité de réactiver un lien en cas de panne pour assurer la continuité du service [18] .

II.4.1.1 Fonctionnement du STP

1. **Élection du Root Bridge :** Le processus débute par l'élection d'un commutateur central appelé Root Bridge. Chaque switch du réseau envoie des messages de type BPDU (Bridge Protocol Data Unit) contenant son identifiant de pont (Bridge ID), composé d'une priorité et d'une adresse MAC. Le switch possédant le Bridge ID le plus faible est désigné comme Root Bridge. Ce commutateur devient le point de référence pour toute la topologie STP
2. **Sélection des meilleurs chemins :** Chaque switch calcule le chemin le plus court (le moins coûteux) pour atteindre le Root Bridge. Le port utilisé pour ce chemin est appelé Root Port. Sur chaque lien, un seul port est désigné comme Designated Port pour transmettre les BPDUs. Les autres ports sont bloqués pour éviter les boucles
3. **Mise en état des ports et convergence :**STP coupe les liens qui créent des boucles dans le réseau. Cela évite les problèmes de diffusion infinie Si un lien tombe en panne, STP active un autre lien pour garder le réseau fonctionnel [18].

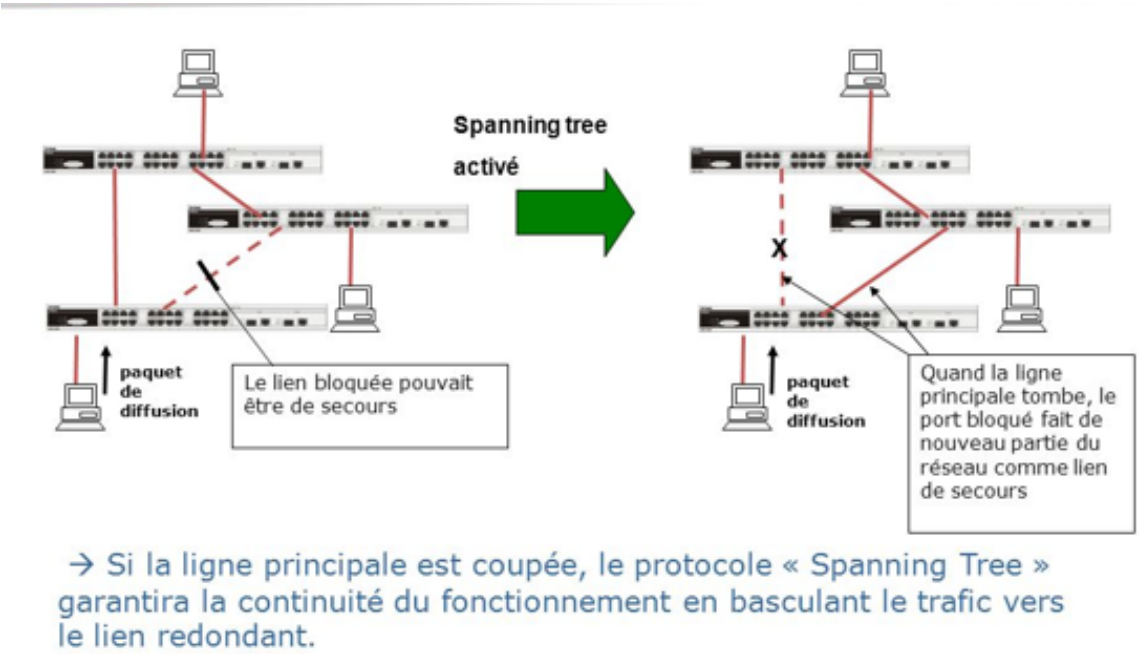

FIGURE II.3 – **Schéma de principe de fonctionnement du STP** [31]

Le protocole STP classique présente une lenteur de convergence, car il ne détecte un changement de topologie qu'après l'expiration de certains temporisateurs, ce qui retarde l'adaptation du réseau. Pour remédier à cette limitation, le protocole RSTP (Rapid Spanning Tree Protocol) a été introduit, offrant une convergence plus rapide en réduisant significativement les délais nécessaires pour réagir aux modifications de la topologie réseau [18].

II.4.2 Le protocole RSTP

RSTP ajoute les rôles de port alternatif, de secours et périphérique, et réduit le nombre d'états de port.il modifie le format BPDU de configuration et utilise le champ « Indicateurs » pour décrire les rôles de port. Il est standardisé par la norme IEEE 802.1W [32].

II.4.2.1 Etat du port du RSTP

Il n'y a plus que trois états pour les ports RSTP :

— Discarding (au lieu de Disabled, Blocking et Listening).

— Learning.

— Forwarding (gardant la même fonction).

Les ports Point-to-Point connectent des commutateurs entre eux. Alors que STP attend passivement des BPDUs pour agir, RSTP négocie le statut des liens rapidement (3 X le Hello Time = 6 secondes) [32].

II.4.3 MSTP (Multiple Spanning Tree Protocol)

Le MSTP est une extension du RSTP qui permet de gérer plusieurs instances de STP sur un même réseau. Chaque instance peut contrôler un ou plusieurs VLAN avec sa propre topologie d'arbre de recouvrement, ce qui optimise l'utilisation des liens et évite les boucles.

MSTP permet de gérer plusieurs VLAN avec des topologies différentes, tout en évitant les boucles et en améliorant l'efficacité du réseau[33].

II.4.3.1 Fonctionnement du MSTP

Regroupement des VLANs en instances (MSTP) Le MSTP permet d'associer plusieurs VLANs à une seule instance de spanning tree, appelée MSTI (Multiple Spanning Tree Instance). Chaque MSTI calcule sa propre topologie, ce qui optimise l'utilisation des liens réseau en répartissant le trafic selon les VLANs.

Définition des régions MSTP Les commutateurs partageant les mêmes paramètres (nom de région, niveau de révision, mappage VLAN-MSTI) forment une région MST. Au sein de chaque région, une instance spéciale appelée IST (Instance Spanning Tree interne) est utilisée pour maintenir la compatibilité avec les réseaux STP/RSTP existants.

Optimisation du trafic et prévention des boucles Chaque MSTI calcule indépendamment sa topologie, permettant une répartition efficace du trafic et évitant les boucles en bloquant les chemins redondants inutiles. Cela assure une meilleure résilience du réseau et une utilisation optimale de la bande passante[33].

II.4.3.2 La comparaison des protocoles STP, RSTP, MSTP

Tableau II.3 résume une étude comparative entre STP et ses variants (RSTP, MSTP).

Protocole Spanning Tree	Vitesse de convergence	Transfert de trafic	Complexité de la configuration
STP (IEEE 802.1D)	Le plus lent	Les VLAN partagent un arbre de recouvrement, à travers lequel tout leur trafic est transféré.	Faible
RSTP (IEEE 802.1W)	Convergence rapide (plus rapide que STP)	Tous les VLAN partagent un arbre de recouvrement, à travers lequel tout leur trafic est transféré.	Faible
MSTP (IEEE 802.1S)	Convergence rapide (équivalente à RSTP)	Grâce au mappage entre les instances et les VLAN, plusieurs spanning trees peuvent équilibrer la charge du trafic. Le trafic de différents VLAN est acheminé par des chemins différents.	Élevée

TABLE II.3 – **Comparaison des protocoles Spanning Tree**
[34]

II.4.4 LACP Link Aggregation Control Protocol)

C'est un protocole de niveau de liaison de données utilisé pour regrouper plusieurs liens logiques en un seul lien physique. Le but principal de LACP est d'améliorer la disponibilité et la bande passante d'une connexion réseau en utilisant plusieurs ports en tant qu'un seul grand port[35].

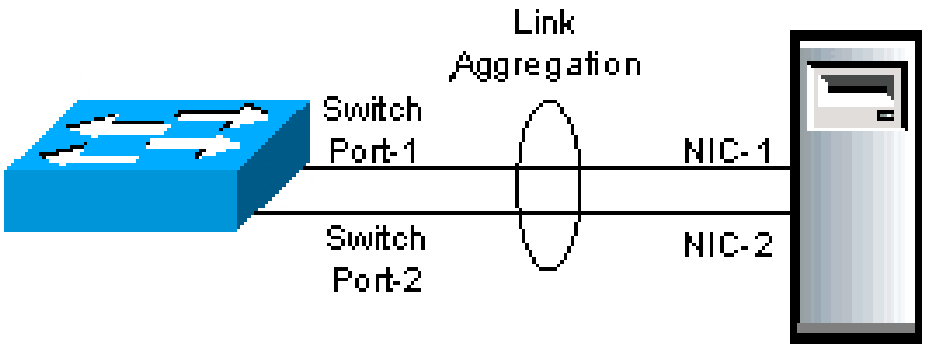

FIGURE II.4 – **Agrégation de liens entre un commutateur et un serveur**
[36]

LACP défini par IEEE 802.3ad est il souvent utilisé avec le Link aggregation pour mettre en œuvre des solutions de tolérance de panne.En utilisant LACP, les équipements réseau peuvent déterminer automatiquement s'ils peuvent former un

LAG.

II.4.4.1 Avantages du lacp

L'agrégation de liens offre les avantages suivants :

— **Fiabilité et disponibilité accrues :** si l'une des liaisons physiques du LAG tombe en panne, le trafic est réaffecté de manière dynamique et transparente à l'une des autres liaisons physiques.

— **Meilleure utilisation des ressources physiques :** le trafic peut être équilibré sur les liaisons physiques.

— **Bande passante accrue :** les liaisons physiques agrégées fournissent une bande passante plus large que chaque liaison individuelle.

— **Rentabilité :** Une mise à niveau du réseau physique peut être coûteuse, surtout si elle nécessite de nouveaux câbles. L'agrégation de liens augmente la bande passante sans nécessiter de nouveaux équipements[35].

II.4.5 EtherChannel

La technologie EtherChannel a initialement été développée par Cisco comme une technique de réseau local entre deux commutateurs permettant d'assembler plusieurs liens physiques Ethernet identiques en un seul lien logique. Cette technologie a pour but d'augmenter la bande passante et d'améliorer la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs [37].

II.4.5.1 Utilité de l'Ether Channel

Comme nous venons de le dire, l'Etherchannel consiste en une agrégation de lien. Le principe est simple, il s'agit de combiner plusieurs liens pour avoir un lien virtuel de meilleure capacité

FIGURE II.5 – **Schéma illustre l'interconnexion de deux switch sans Etherchannel** [38]

Sur la figure ci-dessus, il existe un lien entre les deux switches. Ces derniers pourront donc communiquer à une vitesse de 100 Mbps. Pour bénéficier d'une

meilleure bande passante, nous pouvons faire une agrégation de lien. Nous aurions alors une topologie représentée dans la figure suivante

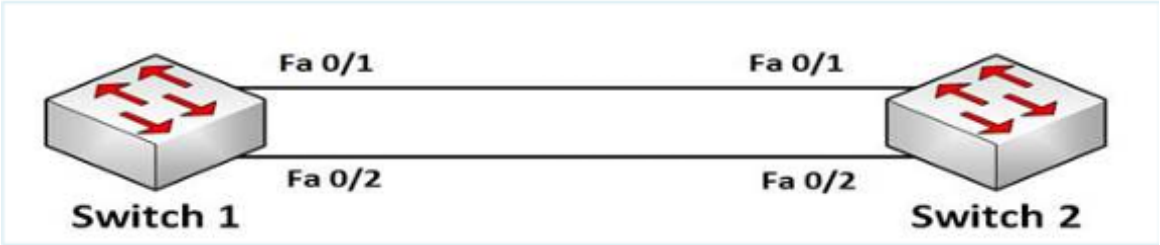

FIGURE II.6 – **Schéma illustre l'interconnexion de deux switch avec Etherchannel** [38]

Sans aucune configuration, STP se chargerait de désactiver l'un des liens. En configurant l'Etherchannel, les deux switches ne verront plus qu'un seul lien virtuel. Ce lien virtuel aura une capacité de 200 Mbps.

II.4.5.2 Avantages de l'Etherchannel

Au moment où un Etherchannel est configuré, l'interface virtuelle résultante est appelée un canal de port. Les interfaces physiques sont regroupées dans une interface de canal de port. Etherchannel présente de nombreux avantages citant [39] :

— La plupart des tâches de configuration peuvent être effectuées sur l'interface EtherChannel plutôt que sur chaque port individuel, ce qui assure la cohérence de la configuration à travers les liens.

— EtherChannel s'appuie sur les ports de commutation existants afin d'augmenter la bande passante. Aucune mise à niveau matérielle n'est nécessaire.

— L'équilibrage de charge est possible entre les liaisons qui font partie d'un même Etherchannel.

— EtherChannel crée une agrégation que STP reconnaît comme une seule liaison logique.

— EtherChannel garante la redondance et la perte d'un lien physique ne génère pas de changement dans la topologie.

II.5 protocole de redondance au niveau du réseau étendu WAN

La redondance au niveau d'un réseau étendu (WAN) est essentielle pour garantir la continuité des services en cas de défaillance. Voici un aperçu des principaux protocoles utilisés pour assurer cette redondance.

II.5.1 BGP (Border Gateway Protocol) : protocole en haute disponibilité

Border Gateway Protocol (BGP) est un protocole d'échange de route externe (un EGP), utilisé notamment sur le réseau Internet. Son objectif principal est d'échanger des informations de routage et d'accessibilité de réseaux (appelés préfixes) entre Autonomous Systems (AS). Comme il circule sur TCP, il est considéré comme appartenant à la couche application du modèle OSI.

Le Border Gateway Protocol (BGP) joue un rôle essentiel dans la mise en œuvre de la haute disponibilité des réseaux, notamment grâce à la technique du multihoming. Cette approche permet à une organisation de maintenir une connectivité continue à Internet, même en cas de défaillance d'un fournisseur d'accès ou d'une liaison. [40].

II.5.1.1 Type du BGP

Il existe deux types de BGP :

— **BGP externe :** il facilite l'échange d'informations de routage entre les routeurs de systèmes autonomes distincts, permettant l'échange transparent de données de routage. Il est également connu sous le nom d'eBGP (External Border Gateway Protocol)[40].

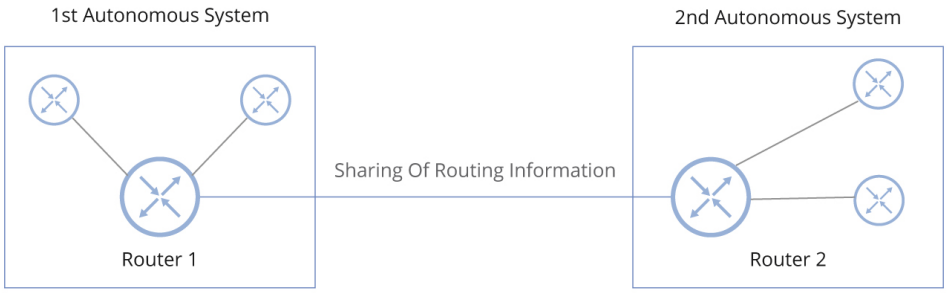

FIGURE II.7 – **BGP Externe**
[41]

— **BGP interne :** Il facilite l'échange d'informations de routage entre les routeurs d'un même système autonome. Il assure la cohérence entre les routeurs internes pour le partage des informations de routage. Il est également connu sous le nom de iBGP (Internal Border Gateway Protocol). [40]

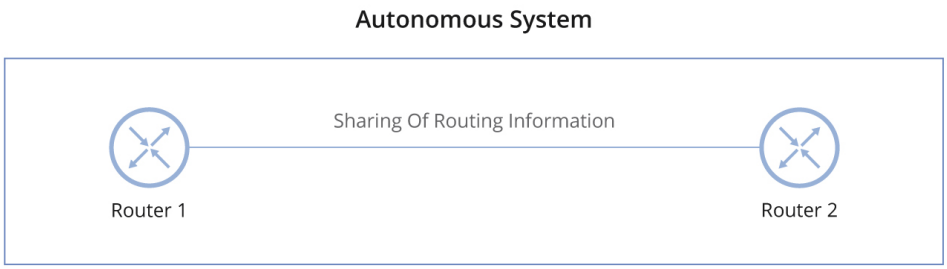

FIGURE II.8 – **BGP interne**
[41]

II.5.1.2 Fonctionnement du BGP

— **Avantages du réseau :** Les routeurs BGP échangent des informations en temps réel, ce qui permet une adaptation rapide aux changements du réseau. Cela garantit une connectivité ininterrompue en cas de défaillance.

— **Optimisation du trafic sur le réseau :** BGP évalue et sélectionne la route la plus appropriée pour diriger le trafic entre les réseaux, garantissant ainsi un routage efficace et des performances optimales du réseau.

— **Amélioration de la connectivité du réseau :** Le protocole BGP permet aux réseaux d'établir des connexions avec plusieurs fournisseurs en amont, ce qui améliore la redondance et les performances.

— **Équilibrage de la charge :** BGP facilite l'équilibrage de la charge en répartissant le trafic sur plusieurs liaisons, ce qui permet d'optimiser les performances du réseau[40].

II.5.2 OSPF (Open Shortest Path First)

SPF est un protocole de routage à état de liens (link-state) utilisé pour acheminer les paquets de données vers leur destination finale. OSPF est connu pour sa convergence rapide, sa fiabilité, sa sécurité et sa flexibilité, ce qui en fait un choix populaire pour les réseaux de toutes tailles [42].

II.5.2.1 Fonctionnement d'OSPF

L'OSPF fonctionne selon plusieurs points essentiels, nous en citons :

— **Échange d'informations de routage :** les routeurs OSPF partagent des informations détaillées sur la topologie du réseau entre eux, créant une base de données commune.

— **Calcul du meilleur chemin :** chaque routeur utilise l'algorithme de Dijkstra pour calculer le chemin le plus court vers toutes les destinations possibles en se basant sur la base de données commune.

— **Tables de routage dynamiques :** les routeurs OSPF peuplent leurs tables de routage avec les chemins les plus optimaux, garantissant un acheminement efficace des paquets.

II.5.2.2 Avantages d'OSPF

Voici quelques-uns de ses principaux avantages :

— Offrir une convergence rapide sans boucles et à chemins multiples.

— OSPF est adapté aux réseaux de grande taille grâce à sa structure hiérarchique et sa capacité à diviser le réseau en zones pour une gestion plus efficace.

— OSPF réagit rapidement aux changements de topologie du réseau, adaptant instantanément les tables de routage et garantissant une continuité de service.

II.6 Conclusion

Dans ce chapitre, nous avons étudié les protocoles de redondance tels que HSRP, VRRP, GLBP pour les équipements, STP, LACP pour le LAN, et BGP, OSPF pour le WAN. Ces protocoles assurent la continuité du service, la tolérance aux pannes et l'optimisation du trafic, garantissant ainsi une infrastructure réseau fiable et performante.

Chapitre III

Mise en oeuvre d'une solution de redondance dans un réseau LAN/WAN

III.1 Introduction

Dans le but de clarifier et de compléter ce qui a été traité dans les chpitre précédents. Ce chapitre présente le groupe Cevital en détaillant ses principaux départements, ainsi que les informations pertinentes en lien avec notre étude.

Nous exposerons ensuite la conception et la mise en œuvre des solutions proposées dans le cadre de notre projet, qui vise à déployer un réseau hautement disponible pour l'entreprise Cevital. Les configurations nécessaires ont été réalisées, notamment celles liées aux VLANs, au VTP, au STP, au HSRP et à l'OSPF, en s'appuyant sur le simulateur Cisco Packet Tracer. Chaque étape sera expliquée de manière claire, illustrée et détaillée.

Enfin, la fiabilité de la solution sera évaluée à l'aide de tests destinés à valider son efficacité.

III.2 Présentation de l'entreprise et de son historique

Cevital Agro-Industrie, filiale du groupe Cevital, est une entreprise privée algérienne fondée en 1998. Implantée dans le port de Béjaïa, elle est détenue majoritairement par la famille Rebrab, avec Issad Rebrab comme fondateur et ses enfants comme principaux actionnaires. Jouant un rôle clé dans le développement du secteur agroalimentaire national, Cevital Agro-Industrie s'est distinguée par son savoir-faire, ses installations de production modernes, un contrôle qualité rigoureux et un vaste réseau de distribution. Grâce à ces atouts, l'entreprise a permis à l'Algérie de passer du statut d'importateur à celui d'exportateur pour des produits tels que les huiles végétales, les margarines et le sucre . Les produits de Cevital Agro-Industrie sont distribués dans plusieurs régions, notamment en Europe, au Maghreb, au Moyen-Orient et en Afrique de l'Ouest, renforçant ainsi la position de l'entreprise en tant que leader dans l'industrie agroalimentaire en Afrique et dans la région méditerranéenne.

FIGURE III.1 – **Logo Cevital**

III.2.1 Situation géographique de Cevital

Cevital Agro-Industrie, le plus grand complexe privé en Algérie, est situé à Béjaïa, près du port et de la route nationale 26, à une distance avantageuse de 280 km d'Alger. Cette localisation stratégique facilite l'accès aux infrastructures clés

telles que l'aéroport, le port et la zone industrielle d'Akbou, offrant ainsi à l'entreprise son propre quai privé. Outre ses installations à Béjaïa, le groupe possède des bureaux dans plusieurs autres villes algériennes. A l'international, Cevital a étendu ses activités avec des bureaux et des installations dans divers pays, où ses filiales se concentrent principalement sur la distribution et la commercialisation des produits Cevital.

FIGURE III.2 – **Vue satellitaire du complexe CEVITAL**

III.2.2 Valeurs du Groupe CEVITAL

Les quatre règles d'or (IRIS) à respecter sont les suivantes

- **Initiative :** le collaborateur doit anticiper les problèmes potentiels et proposer des solutions innovantes grâce à sa connaissance du métier.
- **Respect :** un principe primordial entre collaborateurs et avec les partenaires internes et externes.
- **Intégrité :** une valeur fondamentale, les collaborateurs doivent adopter une éthique professionnelle irréprochable à travers leurs actions.
- **Solidarité :** les collaborateurs doivent s'entraider mutuellement et partager leurs expériences et leurs connaissances.

III.2.3 Présentation du service informatique

Nous avons effectué notre stage au niveau de département Réseau et Télécom de la direction des systèmes d'information (DSI),cette dernière assure la mise en oeuvre des moyens et des technologies de l'information nécessaire pour améliorer

l'activité ,la stratégie et la performance de l'entreprise, elle doit ainsi veiller à la cohérence des moyens informatiques et de la communication mises à la disposition des utilisateurs, à leur maîtrise technique et à leur disponibilité et opérationnalité permanentes et ce en toute sécurité. Figure 89 montre l'organigramme du système d'information.

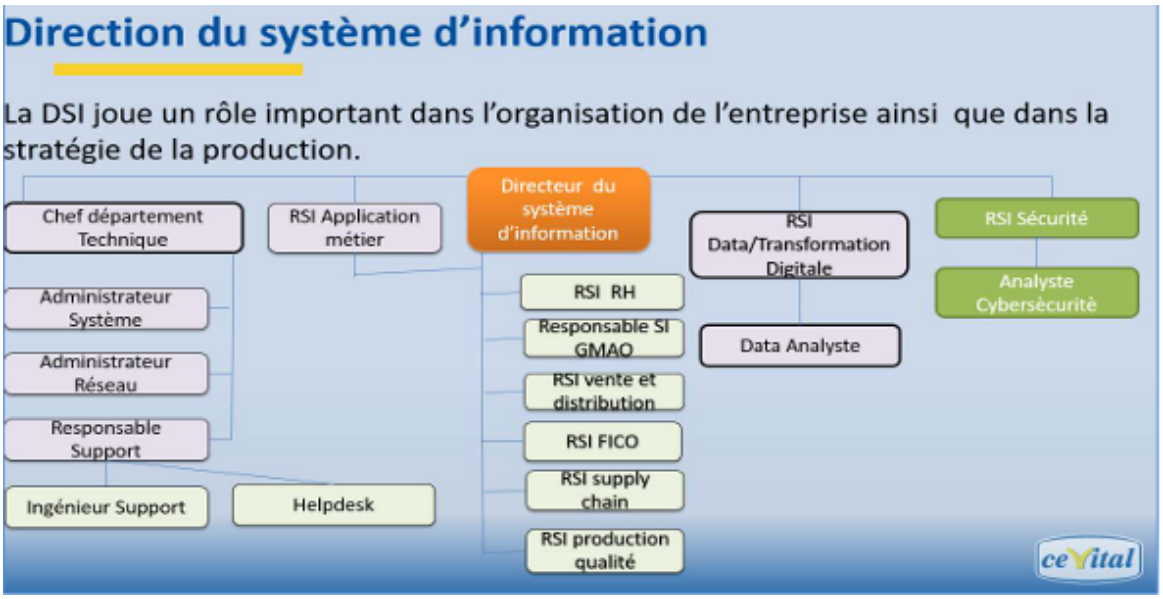

FIGURE III.3 – **Organigramme de la direction système d'information Organigramm**

Le service informatique est suivi par des responsables spécialistes cités ci-dessous :

- **Directeur du système d'information :** Il est chargé de résoudre les problèmes informatiques rapidement et à moindre coût. Il choisit aussi des solutions pour améliorer le travail et la productivité de l'entreprise.
- **Administrateur système :** Il installe et s'occupe du bon fonctionnement des ordinateurs et des systèmes dans l'entreprise. Il gère aussi la maintenance des systèmes utilisés sur le réseau.
- **Administrateur réseau :** Il s'occupe du réseau pour que les informations circulent bien dans l'entreprise. Il veille à la qualité, la continuité et la performance du réseau et du matériel, tout en répondant aux besoins des utilisateurs.
- **Responsable support :** Il contrôle à distance les ordinateurs, aide les utilisateurs à utiliser leur matériel et assure un support par téléphone à l'intérieur de l'entreprise.

III.3 Architecture réseau de Cevital

CEVITAL dispose d'un réseau interne assez vaste permettant de relier les différents bâtiments, unités de production et direction de complexe. Il peut être

structuré en plusieurs composantes : le backbone du réseau, un pare-feu et un DMZ (zone démilitarisée), une couverture wifi, un routeur et un data-center (où sont placés les serveurs de l'entreprise). Le réseau est composé de plusieurs équipements dont la plupart sont de marque Cisco interconnectés entre eux grâce à la fibre optique ou câbles en cuivre.

Le réseau local du complexe se compose de trois couches, couche coeur qui représente aussi la couche distribution (backbone), la couche accès et la couche en cascade.

- **Couche coeur :** le Backbone est composé d'un Switch Catalyst placé au data center du bâtiment, qui est relié aussi bien au pare feu et au routeur à l'aide des câble RJ45, qu'aux Switch d'accès à l'aide de la fibre optique assurant ainsi une bande passante optimale pour les différents postes. Cette partie est la plus sensible parce qu'elle est reliée à tous les équipements réseau.
- **Couche d'accès :** Cette couche se compose des switches qui sont distribués sur les différents sites locaux du bâtiment. Les responsables du réseau de CEVITAL utilisent des Vlans pour partager l'accès aux utilisateurs d'une façon que chaque site local (étage des bâtiments) comprend un ou plusieurs Vlans
- **Couche en cascade :** Dans cette couche les switches sont interconnectés entre eux et aux switches d'accès et assurant la connectivité aux utilisateurs, au sein de ses switches des Vlans permettent de définir plusieurs sous réseaux en fonctions des départements de l'entreprise.

  Cevital utilise des commutateurs des modèles 2960X et 2960L, comme représenté dans la figure ci-dessous. On y trouve un total de 45 switchs.

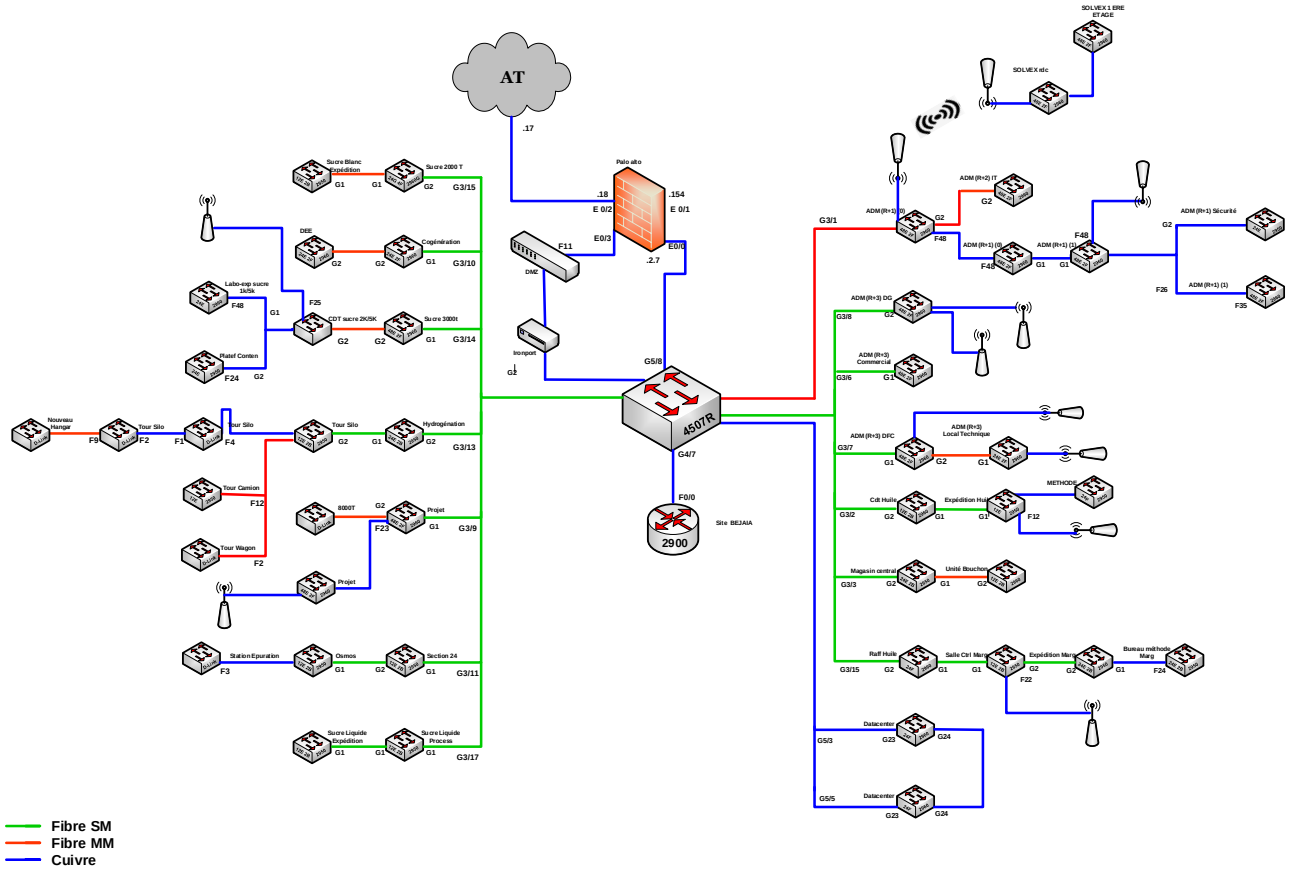

FIGURE III.4 – **Architecture réseau LAN de Cevital**

III.3.0.1 Liaisons inter- sites (architecture WAN)

Afin d'assurer une communication fluide et un partage efficace des ressources, CEVITAL a établi des connexions entre son site de Bejaïa et plusieurs sites distants de l'entreprise incluant notamment :

— Une liaison spéciale fibre optique entre le site distant et le site de bejaia via un fournisseur d'accés (Algerie Telecom).

— Une liaison faisceau hertzien (FH) entre le site distant et le site de bejaia via un fournisseur d'accés (Algerie Telecom).

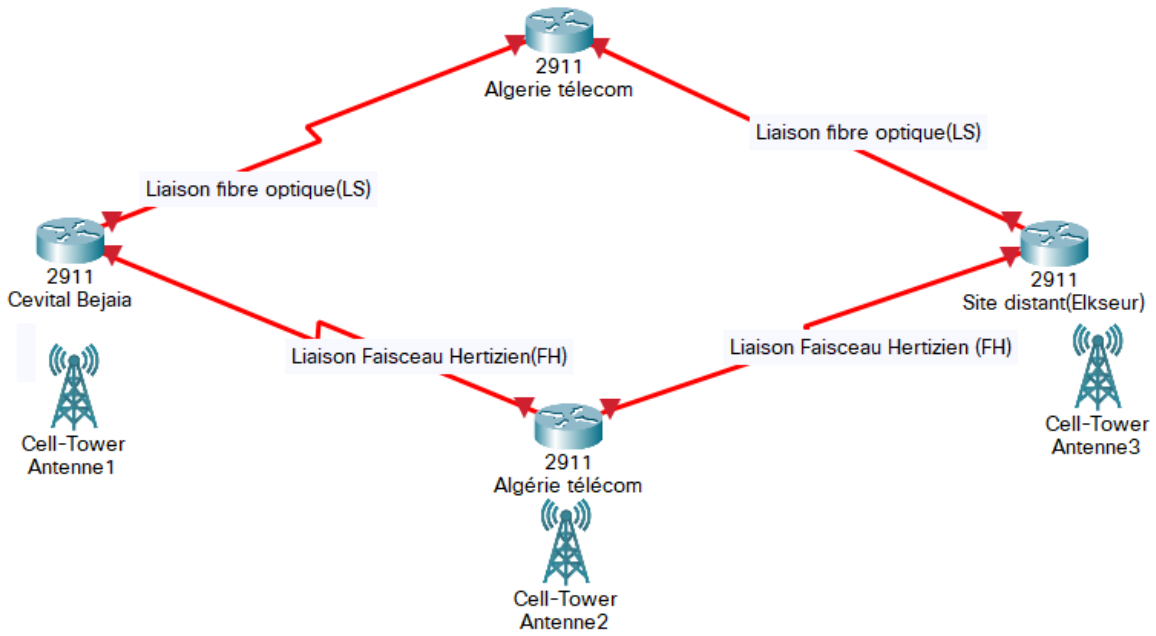

FIGURE III.5 – **Lisaison inter-sites du groupe Cevital**

III.3.1 Matériels utilisés dans l'architecture réseau :

le réseau est composé de plusieurs dispositifs dont la plupart sont de marque Cisco (Switch Catalyst, Routeur) interconnectés entre eux au moyen de liaisons en fibre optique ou de câbles à paires torsadées en cuivre.

— **Distributeur (Backbone) de type Cisco Catalyst 4507R :** aussi appelé switch fédérateur, il assure la gestion du trafic principal du réseau de cevital. Il relie les commutateurs d'accès, le pare-feu, les serveurs et les routeurs. Il prend en charge le routage inter-VLANs, permet l'accès à l'nternet via le pare-feu et occupe fréquemment le rôle de serveur DHCP.

FIGURE III.6 – **Switch distributeur Cisco Catalyst 4507R.**

— **Switch d'accès et en cascade de type Cisco Catalyst 2960X et 2960L :** ils sont connectés au backbone et installés dans les différents bâtiments de l'entreprise.

FIGURE III.7 – **Switch Cisco Catalyst 2960**

— **Routeur de type Cisco 2900 :** il permet de gérer le routage entre les différents sites de l'entreprise.

FIGURE III.8 – **Routeur Cisco 2900 .**

— **Point d'accès wi-fi :** l'entreprise dispose de plusieurs points d'accès wi-fi, créant ainsi une couverture réseau sans fil au niveau de certaines parties du complexe.

FIGURE III.9 – **Point d'accès wi-fi Ruckus**

— **Pare-feu :** deux pare-feux sont reliés en redondance et assurant la sécurisation du réseau, d'isoler certaines parties de celui-ci et le contrôle de l'accès à internet.

FIGURE III.10 – **Pare-feu**

— **Data center :** le data center est une salle sécurisée avec un accès limité aux responsables et techniciens de la DSI. Il est climatisé et équipé d'une double alimentation électrique afin de prévenir les coupures. C'est le centre du réseau de cevital, où se trouvent les serveurs, backbones, pare-feu, routeurs et le standard téléphonique de l'entreprise.

FIGURE III.11 – **Data Center**

III.3.2 Nombre et modèles des Switchs

Cevital utilise des commutateurs des modèles 2960X et 2960L, comme illustré dans la figure III.4. On y trouve un total de 45 switchs.

III.3.3 Nombre et modèles des Serveurs

Cevital dispose de 90 serveurs, dont certains sont physiques, tandis que les autres sont des machines virtuelles, dont :

— Serveur WSUS pour les mises à jour des machines.

— Sage x3 pour la facturation et la comptabilité.

— Coswin pour la gestion des stocks et maintenance

— Kelio pour le suivi des pointages.

— Skeeper pour la traçabilité.

— 2 Exchange comme serveurs de messagerie.

— GLPI présente la plateforme pour recevoir les tickets des utilisateurs en cas de problèmes informatiques.

III.3.4 Codification des équipements de Cevital

— CEVWKS 1XXX : ordinateur de bureau.

— CEVLAP 1XXX : ordinateur portable.

— CEVSRV 1XXX : serveur.

— CEVAP 1XX : switch.

— CEVAP 1XXX : point d'accès wifi.

— CEVFW 1XXX : pare-feu.

— CEVRTR 1XXX : routeur.

III.3.5 VLANs de l'entreprise

L'administrateur réseau a divisé le réseau en plusieurs VLANs selon différentes divisions, un VLAN management a été créé pour permettre l'administration (configuration, mise à jour et équipement de sauvegarde) du réseau distant

III.4 La mise en place d'un réseau LAN redondant

III.4.1 Optimisation de la conception

Afin d'assurer la redondance et la haute disponibilité, nous avons apporté des améliorations à l'ancienne architecture réseau de Cevital, ses améliorations concernent les deux couches principales du réseau de l'entreprise : la couche cœur et la couche d'accès.

Direction	**VLAN**	**Direction**	**VLAN**
Server 1	2	ICOSNET-VPN	3
DRH	10	Achats	11
IT	12	Huile	13
Sucre3000T	14	Utilité	15
Supply-chain	16	Margarinerie	17
Printer	18	Server 2	19
PABX	20	Visio	21
Direction R&D	22	Performance industrielle	23
Conditionnement Huile	24	Management	25
DFC	26	Commercial	27
QHSE	29	Sucre3500T	30
Camera IP	32	Marketing	34
Solvex	36	GUEST	41
Contrôle Accès	43	Imprimante Domino	45
Monitoring DC	48	Srv-collaboration	60
Srv-production	62	Srv-BDD	63
Srv-backup	64	Srv-ESXI	65
rv-preprod	66	Serveurs-securite	67
WAN-RMS	70	WAN-VSAT	71
Firewall-Datacenter	72	Firewall-frontaux	73
MGMT-Tor	74	Test	75
CCTV	80	Industriel	81

TABLE III.1 – **Affectation des VLANs aux directions triées par VLAN**

Pour garantir une redondance de passerelle nous avons mis en œuvre deux switchs dans la partie cœur afin de configurer le protocole de HSRP sur ces deux équipements. Ces switches sont interconnectés via une liaison EtherChannel, dans le but d'améliorer la connectivité et d'assurer un débit élevé.

Voici les deux couches principales de l'architecture :

— **Couche cœur :** à ce niveau, nous avons ajouté un second switch, SWC2, afin de partager la charge du trafic réseau avec SWC1. En cas de panne de l'un

des deux, l'autre prend automatiquement le relais pour assurer la continuité du service.

— **Couche d'accès :** nous avons conservé l'ancienne structure, Chaque switch d'accès est relié aux switches cœur selon deux schémas de connexion différents afin de maintenir un faible diamètre réseau.

Sur la couche cœur, nous avons configuré plusieurs protocoles essentiels : SSH pour un accès sécurisé, pour assurer la redondance des liens, nous avons configuré le protocole STP afin d'éviter les boucles dans le réseau. Ensuite nous avons réparti les rôles de root bridge entre les deux équipements pour équilibrer le trafic (SWC1 est défini comme root bridge pour les vlans 2 à 6 et comme route secondaire pour les vlans 7 à 12 pour le SWC2 c'est l'inverse). Afin de séparer les flux, nous avons mis en place le protocole VTP pour la gestion des VLANs, y compris sur la couche d'accès, et configuré le protocole HSRP afin d'assurer une haute disponibilité.

Enfin, le protocole de routage dynamique OSPF est mis en place à la fois sur le routeur et sur les switchs de la couche cœur. Il assure un routage efficace et dynamique à travers le réseau. L'ensemble de cette configuration garantit la continuité des services réseaux même en cas de panne d'un switch de coeur ou d'une coupure de lien, grâce à la redondance des connexions entre la couche d'accès et les deux switchs de cœur.

Afin de simplifier l'architecture réseau, nous avons opté pour l'utilisation de seulement six switchs d'accès. Chaque switch est dédié à un segment spécifique du réseau local (LAN).

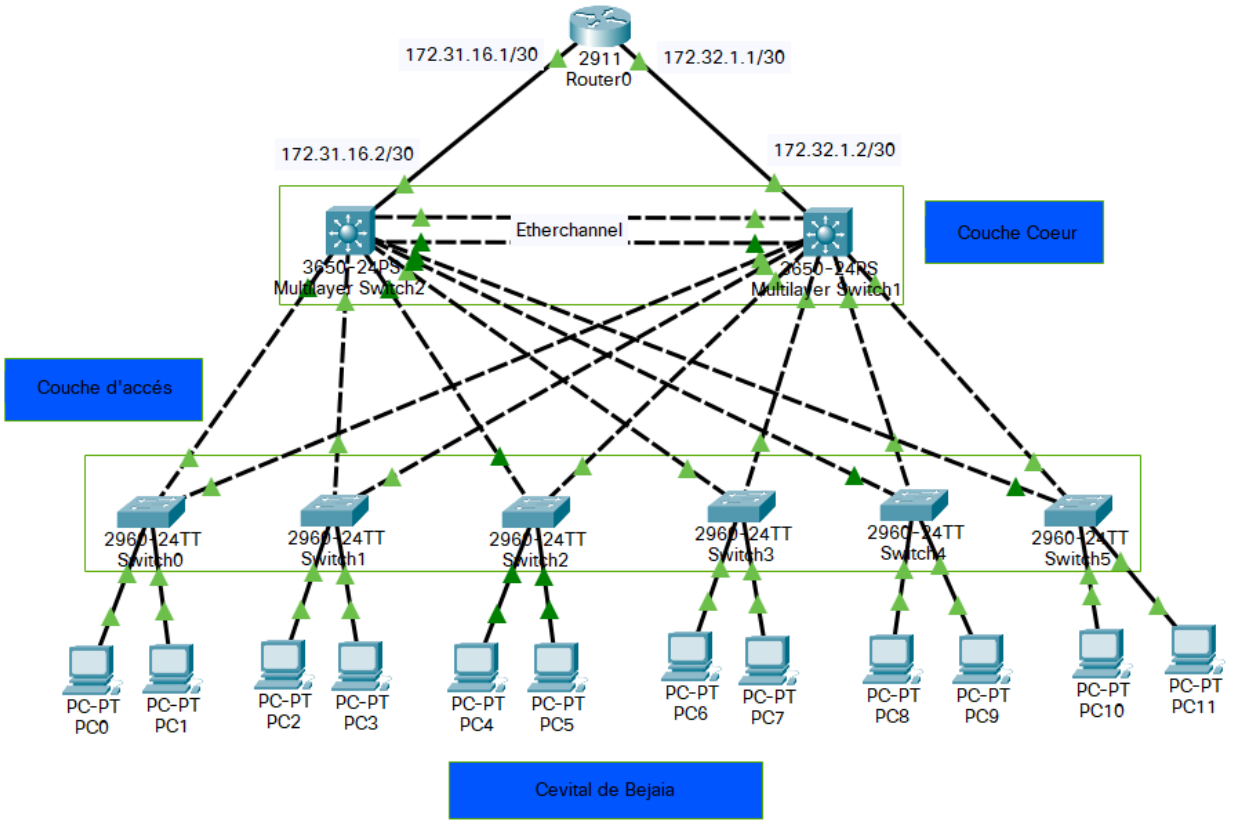

FIGURE III.12 – **Topologie de la nouvelle architecture de réseau LAN de cevital**

III.4.2 Présentation des équipements utilisés

Equipements	Modèle d'équipement	Nombre	Nomination
Couche coeur	Switch coeur (WS-C3650-24PS)	2	SWC1 SWC2
Couche d'accès	Switch Cisco WS-C2960-24TT	6	SWAn n = 1...6
Routeur	Router Cisco 2911	1	Router
PCs	PC-PT	12	PCn

TABLE III.2 – **Les équipements utilisés sur la topologie**

Équipement Local	Équipement Distant	Interface(s) Locale(s)	Interface(s) Distante(s)
Routeur	Coeur1	Gig0/0	Gig1/0/1
Routeur	Coeur2	Gig0/1	Gig1/0/1
Coeur1	Coeur2	Gig1/0/8-Gig1/0/9	Gig1/0/8-Gig1/0/9
Coeur1	SWA1	Gig1/0/2	Fa0/1
Coeur1	SWA2	Gig1/0/3	Fa0/1
Coeur1	SWA3	Gig1/0/4	Fa0/1
Coeur1	SWA4	Gig1/0/5	Fa0/1
Coeur1	SWA5	Gig1/0/6	Fa0/1
Coeur1	SWA6	Gig1/0/7	Fa0/1
Coeur2	SWA1	Gig1/0/2	Fa0/2
Coeur2	SWA2	Gig1/0/3	Fa0/2
Coeur2	SWA3	Gig1/0/4	Fa0/2
Coeur2	SWA4	Gig1/0/5	Fa0/2
Coeur2	SWA5	Gig1/0/6	Fa0/2
Coeur2	SWA6	Gig1/0/7	Fa0/2

TABLE III.3 – **Désignation des interfaces**

III.4.3 Désignation des interfaces

III.4.4 VLANs utilisés dans la topologie LAN

Direction	VLAN	Adresse réseau	Passerelle	DHCP	Root	IP SWC1	IP SWC2
IT	VLAN 2	10.90.2.0	10.90.2.254	Dynamique	SWC1	10.90.2.252	10.90.2.253
DFC	VLAN 3	10.90.3.0	10.90.3.254	Dynamique	SWC1	10.90.3.252	10.90.2.253
DRH	VLAN 4	10.90.4.0	10.90.4.254	Dynamique	SWC1	10.90.4.252	10.90.4.253
RH (Raff Huile)	VLAN 5	10.90.5.0	10.90.5.254	Dynamique	SWC1	10.90.5.252	10.90.5.253
RS (Raff Sucre)	VLAN 6	10.90.6.0	10.90.6.254	Dynamique	SWC1	10.90.6.252	10.90.6.253
SL	VLAN 7	10.90.7.0	10.90.7.254	Dynamique	SWC2	10.90.7.252	10.90.7.253
Imprimante	VLAN 8	10.90.8.0	10.90.8.254	Statique	SWC2	10.90.8.252	10.90.8.253
LOG	VLAN 9	10.90.9.0	10.90.9.254	Dynamique	SWC2	10.90.9.252	10.90.9.253
Téléphone	VLAN 10	10.90.10.0	10.90.10.254	Dynamique	SWC2	10.90.10.252	10.90.10.253
Serveur	VLAN 11	10.90.11.0	10.90.11.254	Statique	SWC2	10.90.11.252	10.90.11.253
Management	VLAN 12	10.90.12.0	10.90.12.254	Statique	SWC2	10.90.12.252	10.90.12.253

TABLE III.4 – **VLAN pour chaque direction**

III.5 Configuration des équipements utilisés

Une fois les équipements interconnectés, il est important de configurer chaque périphérique pour établir un réseau redondant. Après avoir appliqué ces configurations, il est essentiel de les sauvegarder afin qu'elles soient conservées même après un redémarrage ou une coupure de courant. Pour ce faire, on utilise la commande suivante : **«copy running-config»**

III.5.0.1 configuration du base :

La même configuration de base sera effectuée sur le routeur,Les switches Cores et les switches d'accès.

III.5.0.2 Hostname :

Pour reconnaître nos équipements, nous commençons par attribuer des noms significatifs avec la commande « **hostname** ».

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SWC1
SWC1(config)#
```

FIGURE III.13 – **Attribution du nom SWC1 au switch Core**

III.5.0.3 Configuration de la ligne Console

Pour sécuriser l'accès aux périphériques nous avons attribué un mot de passe « telecom » pour la ligne console de chaque commutateur de niveau 2 et 3.

```
SWC1(config)#line con 0
SWC1(config-line)#password telecom
SWC1(config-line)#login
SWC1(config-line)#exit
SWC1(config)#
```

FIGURE III.14 – **Configuration de line console.**

III.5.0.4 Sécurisation du mode privilégié

Nous avons attribué un mot de passe « telecom » pour l'accès au mode privilégié.

```
SWC1(config)#enable password telecom
SWC1(config)#
```

FIGURE III.15 – **Attribution d'un mot de passe pour l'accès au mode privilégiée.**

III.5.0.5 Sécurisation des mots de passe

Les mots de passe apparaissent en clair lors de l'affichage du fichier de configuration. Nous allons donc activer le service password encryption afin de sécuriser les équipements.

```
User Access Verification

Password:

SWC1>en
Password:
SWC1#sh ru
SWC1#sh running-config
Building configuration...

Current configuration : 5614 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SWC1
!
!
enable password telecom
!
```

FIGURE III.16 – **curation des mots de pass**

III.5.0.6 Configuration d'une bannière :

Nous avons utilisé une bannière de type « banner motd » qui indique que cet accès est interdit aux utilisateurs non autorisés (Hackers).

```
SWC1(config)#banner motd " Acces aux personnes autorisees "
SWC1(config)#
```

FIGURE III.17 – **Configuration d'une bannière motd.**

III.5.0.7 Securisation d'accès à distant avec SSH

est largement utilisé par les administrateurs réseau pour gérer à distance les systèmes et les applications en toute sécurité,Il leur permet de se connecter à un autre ordinateur sur un réseau, d'exécuter des commandes et de déplacer des fichiers d'un ordinateur à un autre.

Nous allons activer le SSH sur les commutateurs de la couche cœur. Voici un exemple des étapes de configuration sur le switch SWC1.

```
SWC1(config)#username Rania password KH012387
SWC1(config)#ip domain-name cisco.com
SWC1(config)#crypto key generate rsa
% You already have RSA keys defined named SWC1.cisco.com .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: SWC1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SWC1(config)#line vty 04
*Mar 1 0:28:59.99: %SSH-5-ENABLED: SSH 1.99 has been enabled
SWC1(config-line)#transport input ssh
SWC1(config-line)#end
```

FIGURE III.18 – **Configuration du SSH sur SWC1**

III.5.0.8 Vérification des configurations de base

La commande « **show running-config** » nous permet de vérifier l'ensemble des configurations effectuées sur l'équipement.

III.5.0.9 Configuration des liaisons Trunk

Dans cette section nous allons configurer les liaisons des switches cores (Niveau 3) en mode trunk. La commande « **interface range** » nous permet de regrouper les interfaces de chaque switch sur SWC1 ET SWC2.

Exemple sur SWC2 :

```
SWC1(config)#interface range gigabitEthernet 1/0/1-8
SWC1(config-if-range)#switchport trunk encapsulation dot1q
SWC1(config-if-range)#switchport mode trunk
```

FIGURE III.19 – **Configuration du trunk sur SWC2.**

Sur les switchs d'accès : Dans cette section nous allons configurer les liaisons des switches d'accès (Niveau 2) en mode trunk.

La commande **«interface range»** nous permet de regrouper les interfaces de chaque switch.

```
SWA1(config)#interface RANG fastEthernet 0/1-2
SWA1(config-if-range)#SWitchport MOde TRunk
SWA1(config-if-range)#EXIT
```

FIGURE III.20 – **Configuration du Trunk sur switch d'accès.**

Vérification des liaisons Trunk : Avec la commande **« show running-config »** sur SWC1 et SWC2 :

```
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/8
 --More--
```

FIGURE III.21 – **Vérification des liens trunks sur « SWC1 »**

III.5.0.10 Configuration des VLANs :

Nous allons créer tous les VLANs de l'entreprise sur le switch Core 1 (SWC1). Prenons exemple pour le Vlan 2 et 3 comme sur la figure suivante :

```
SWC1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWC1(config)#vlan 2
SWC1(config-vlan)#name IT
SWC1(config-vlan)#EXIT
SWC1(config)#VLAN 3
SWC1(config-vlan)#name DFC
SWC1(config-vlan)#
```

FIGURE III.22 – **Création des VLANs sur SWC1**

Vérification de la création des VLANs Avec la commande **« show vlan brief »**.

```
SWC1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/1, Gig1/0/9, Gig1/0/10, Gig1/0/1
                                                Gig1/0/12, Gig1/0/13, Gig1/0/14,
Gig1/0/15
                                                Gig1/0/16, Gig1/0/17, Gig1/0/18,
Gig1/0/19
                                                Gig1/0/20, Gig1/0/21, Gig1/0/22,
Gig1/0/23
                                                Gig1/0/24, Gig1/1/1, Gig1/1/2, Gig1/1/3
                                                Gig1/1/4
2    IT                               active
3    DFC                              active
4    DRH                              active
5    RH                               active
6    RS                               active
7    SL                               active
8    IMPR                             active
9    LOG                              active
10   TEL                              active
11   SERVEUR                          active
12   MANAGMENT                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SWC1#
```

FIGURE III.23 – **Vérification de la création des VLANs.**

III.5.0.11 Configuration du VTP

Afin de profiter des services VTP (création, suppression, modification des Vlans), Nous allons donc configurer le switch de Core « SWC1 » en mode Serveur et lui attribué un nom de domaine ainsi un mot de passe, et le reste des switches en mode Client afin que les Vlans se propagent du SWC1 vers les autres switches. Pour cela nous allons procéder comme suit : Configurer le SWC1 en VTP serveur :

```
SWC1(config)#vtp mode server
Setting device to VTP SERVER mode.
SWC1(config)#vtp domain cevital.dz
Domain name already set to cevital.dz.
SWC1(config)#vtp pass
SWC1(config)#vtp password telecom
Password already set to telecom
SWC1(config)#end
```

FIGURE III.24 – **Configuration de VTP serveur**

Nous allons vérifier cette configuration avec la commande **show vtp status :**

```
SWC1#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : cevital.dz
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0002.17E1.0D00
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 10.90.2.252 on interface Vl2 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 16
Configuration Revision          : 529
MD5 digest                      : 0xDA 0x41 0x86 0xC7 0x91 0x51 0x5B 0x24
                                  0x63 0xB4 0x3B 0x1E 0x69 0x40 0xC1 0xB3

SWC1#
```

FIGURE III.25 – **Vérification de la configuration de VTP serveur.**

Configurer SWC2 en mode client nous allons configurer le switch Core SWC2 en mode Client.

```
SWC2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWC2(config)#vtp domain cevital.dz
Domain name already set to cevital.dz.
SWC2(config)#vtp password telecom
Setting device VLAN database password to telecom
SWC2(config)#vtp version 2
Cannot modify version in VTP client mode
SWC2(config)#
```

FIGURE III.26 – **Configuration de VTP client**

Nous allons aussi vérifier cette configuration avec la commande show vtp status :

```
SWC2#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : cevital.dz
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0009.7C45.8500
Configuration last modified by 0.0.0.0 at 3-1-93 00:39:20

Feature VLAN :
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 16
Configuration Revision            : 1
MD5 digest                        : 0x41 0xF8 0x2F 0x4A 0x64 0x89 0x26 0xAE
                                    0x88 0x1E 0x38 0x83 0xCB 0xA3 0xF3 0x43
SWC2#
```

FIGURE III.27 – **Vérification de la configuration VTP client.**

Configurer les autres Switches niveau accès en mode VTP client :

```
SWA1(config)#VTP MODE CLIENT
Device mode already VTP CLIENT.
SWA1(config)#VTP DOMAIN cevital.dz
Domain name already set to cevital.dz.
SWA1(config)#vtp password telecom
Password already set to telecom
SWA1(config)#end
```

FIGURE III.28 – **Exemple de configuration VTP client sur le Switch accès.**

On vérifie aussi cette configuration avec la commande **show vtp status :**

```
SWA2#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0090.0C90.4000
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN :
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x02 0xD8 0x85 0xD1 0xF5 0x2A 0x29 0x98
                                    0x58 0x57 0xAA 0x7D 0x29 0x08 0xC5 0x47
SWA2#01:43:27 %DTP-5-DOMAINMISMATCH: Unable to perform trunk negotiation on
port Fa0/1 because of VTP domain mismatch.

01:43:27 %DTP-5-DOMAINMISMATCH: Unable to perform trunk negotiation on port
Fa0/2 because of VTP domain mismatch.
```

FIGURE III.29 – **Vérification de la configuration VTP client sur le Switch accès**

III.5.0.12 Attribution des ports aux différents VLANs

Dans cette étape nous allons assigner des ports aux VLANs au niveau des switches d'accès avec les commandes citées dans la figure ci-dessous

```
SWA1(config)#interface range fastEthernet 0/3-4
SWA1(config-if-range)#switchport mode access
SWA1(config-if-range)#switchport access vlan 2
```

FIGURE III.30 – **Exemple d'attribution de port au VLAN 2**

En utilisant la commande «show running-config» pour vérifier la configuration du mode access sur le Switch Accés par exemple.

```
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 2
 switchport mode access
!
```

FIGURE III.31 – **Vérification de la configuration du mode accès sur le switch SWA1**

Nous allons maintenant vérifier si les ports sont bien attribués avec la commande **Show vlan brief.**

```
SWA1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
2    IT                               active    Fa0/3, Fa0/4
3    DFC                              active
4    DRH                              active
5    RH                               active
6    RS                               active
7    SL                               active
8    IMPR                             active
9    LOG                              active
10   TEL                              active
11   SERVEUR                          active
12   MANAGMENT                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

FIGURE III.32 – **Vérification si les VLANs ont bien été propagés.**

III.5.0.13 Configuration des liens EtherChannel

Dans l'architecture, nous avons opté pour une agrégation des liens GigaEthernet entre les deux switchs de Core SWC1 et SWC2, on a donc mis les deux ports GigaEthernet dans un groupe en précisant le mode **ON**, puis on les a mis en mode **trunk** comme le montre :

```
SWC1(config)#INterface Range GigabitEthernet 1/0/8-9
SWC1(config-if-range)#channel-group 1 mode on
SWC1(config-if-range)#
```

```
SWC1(config)#INterface POrt-channel 1
SWC1(config-if)#SWitchport TRunk ENcapsulation Dot1q
SWC1(config-if)#SWitchport Mode Trunk
SWC1(config-if)#EXIT
```

FIGURE III.33 – **Configuration de l'EtherChannel sur SWC1.**

La commande **show etherchannel summary** est utilisée pour vérifier la configuration d'un EtherChannel sur les switches SWC1 et SWC2 :

```
SWC1#SHow ETherchannel Summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------

1      Pol(SD)           -      Gig1/0/8(s) Gig1/0/9(s)
SWC1#
```

FIGURE III.34 – **Vérification de la configuration d'Etherchannel sur le SWC1**

III.5.0.14 Configurations du protocole STP :

Pour faciliter la mise en place d'un chemin logique sans boucle sur l'ensemble du domaine de diffusion nous allons configurer le protocole STP.

III.5.0.14.1 La configuration du l'ID du pont : On commence par l'activation du spanning-tree en tapant la commande «spanning-tree mode pvst» Ensuite, On force le commutateur SWC1 d'être le root bridge de VLAN 2 jusqu'à VLAN 6 et le root bridge de secours de VLAN 7 jusqu'à VLAN 12

```
SWC1(config)#SPAnning-tree MOde PVST
SWC1(config)#SPanning-tree VLan 2-6 PRiority 4096
SWC1(config)#SPanning-tree VLan 7-12 PRiority 8192
SWC1(config)#EXIT
SWC1#
```

FIGURE III.35 – **Configuration du STP sur SWC1**

Nous avons procédé la même chose pour le SWC2, qui est le root bridge du VLAN 7 jusqu'à vlan 12 et le root bridge de secours du VLAN 2 jusqu'a VLAN 6.

```
SWC2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWC2(config)#spanning-tree mode pvst
SWC2(config)#spanning-tree vlan 7-12 PRiority 4096
SWC2(config)#SPanning-tree VLAN 2-6 Priority 8192
SWC2(config)#
```

FIGURE III.36 – **Configuration du STP sur SWC2**

Et nous allons vérifier cette configuration avec la commande **Show running-config :**

```
spanning-tree mode pvst
spanning-tree vlan 2-6 priority 4096
spanning-tree vlan 7-12 priority 8192
!
```

FIGURE III.37 – **Vérification du STP sur SWC1**

```
.
spanning-tree mode pvst
spanning-tree vlan 7-12 priority 4096
spanning-tree vlan 2-6 priority 8192
!
```

FIGURE III.38 – **Vérification du STP sur SWC2**

Pour vérifier la configuration de chaque instance Spanning-tree (c'est-à-dire pour chaque VLAN) en tapant la commande « **show spanning-tree** »

```
VLAN0002
  Spanning tree enabled protocol ieee
  Root ID     Priority    4098
              Address     000D.BDB1.C149
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4098  (priority 4096 sys-id-ext 2)
              Address     000D.BDB1.C149
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
```

FIGURE III.39 – **Instance STP (exemple Vlan 2).**

III.5.1 Configuration du DHCP :

Afin de faciliter la gestion et l'attribution des adresses IP pour chaque hôte du réseau, nous allons utiliser le protocole DHCP, ce dernier permet de configurer les paramètres de chaque hôte et le laissera profiter d'un adressage dynamique. La configuration se fera au niveau des switchs de Core SWC1 et SWC2. Afin de réussir ce protocole, nous allons exclure les adresses de 125 à 251 sur le SWC1, c'est-à-dire que le SWC1 va attribuer les adresses allant de 1 jusqu'à 124.

```
hostname SWC1
!
!
enable password telecom
!
!
ip dhcp excluded-address 10.90.2.125 10.90.2.251
ip dhcp excluded-address 10.90.3.125 10.90.3.251
ip dhcp excluded-address 10.90.4.125 10.90.4.251
ip dhcp excluded-address 10.90.5.125 10.90.5.251
ip dhcp excluded-address 10.90.6.125 10.90.6.251
ip dhcp excluded-address 10.90.7.125 10.90.7.251
ip dhcp excluded-address 10.90.8.125 10.90.8.251
ip dhcp excluded-address 10.90.9.125 10.90.9.251
ip dhcp excluded-address 10.90.10.125 10.90.10.251
ip dhcp excluded-address 10.90.11.125 10.90.11.251
ip dhcp excluded-address 10.90.12.125 10.90.12.251
!
```

FIGURE III.40 – **Les adresses exclues 125-251 sur SWC1.**

Avec la même commande nous vérifions aussi les adresses exclues sur le switch SWD2

```
SWC2(config)#ip dhcp excluded-address 10.90.2.1 10.90.2.124
SWC2(config)#ip dhcp excluded-address 10.90.3.1 10.90.3.124
SWC2(config)#ip dhcp excluded-address 10.90.4.1 10.90.4.124
SWC2(config)#ip dhcp excluded-address 10.90.5.1 10.90.5.124
SWC2(config)#ip dhcp excluded-address 10.90.6.1 10.90.6.124
SWC2(config)#ip dhcp excluded-address 10.90.8.1 10.90.7.124
SWC2(config)#ip dhcp excluded-address 10.90.9.1 10.90.9.124
SWC2(config)#ip dhcp excluded-address 10.90.10.1 10.90.10.124
SWC2(config)#ip dhcp excluded-address 10.90.11.1 10.90.11.124
SWC2(config)#ip dhcp excluded-address 10.90.12.1 10.90.12.124
```

FIGURE III.41 – **Les adresses exclues 1-124 sur SWC2.**

Nous allons créer maintenant un pool d'adresse pour chaque VLAN.

```
SWC1(config)#ip dhcp pool vlan2
SWC1(dhcp-config)#network 10.90.2.0 255.255.255.0
SWC1(dhcp-config)#default-router 10.90.2.254
SWC1(dhcp-config)#exit
SWC1(config)#
```

FIGURE III.42 – **Exemple de création d'un Pool pour le VLAN 2 sur le SWC1**

Nous allons vérifier la création de nos pools DHCP avec la commande **show running-config**

```
!
ip dhcp pool vlan2
 network 10.90.2.0 255.255.255.0
 default-router 10.90.2.254
ip dhcp pool vlan3
 network 10.90.3.0 255.255.255.0
 default-router 10.90.3.254
ip dhcp pool vlan4
 network 10.90.4.0 255.255.255.0
 default-router 10.90.4.254
ip dhcp pool vlan5
 network 10.90.5.0 255.255.255.0
 default-router 10.90.5.254
ip dhcp pool vlan6
 network 10.90.6.0 255.255.255.0
 default-router 10.90.6.254
ip dhcp pool vlan7
 network 10.90.7.0 255.255.255.0
 default-router 10.90.7.254
ip dhcp pool vlan8
 network 10.90.8.0 255.255.255.0
 default-router 10.90.8.254
ip dhcp pool vlan9
 network 10.90.9.0 255.255.255.0
 default-router 10.90.9.254
ip dhcp pool vlan10
 network 10.90.10.0 255.255.255.0
 default-router 10.90.10.254
ip dhcp pool vlan11
 network 10.90.11.0 255.255.255.0
 default-router 10.90.11.254
ip dhcp pool vlan12
 network 10.90.12.0 255.255.255.0
!
```

FIGURE III.43 – **Vérification de la création des pools DHCP**

Après la configuration du DHCP, nous allons configurer les PC pour qu'ils obtiennent une adresse IP automatiquement via DHCP.

Sur le PC0 interconnecté au Vlan 2 :

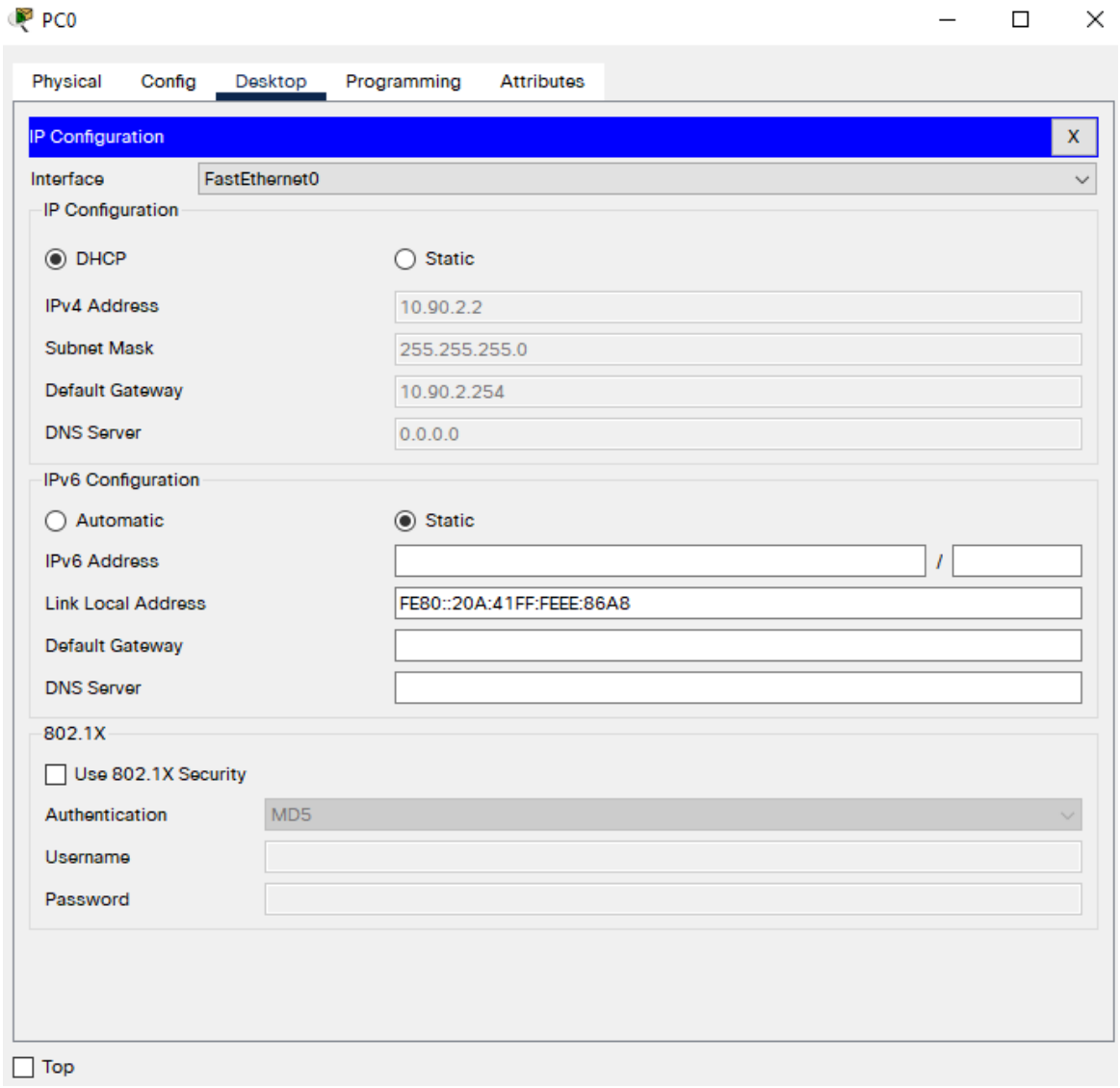

FIGURE III.44 – **vérification du DHCP sur le PC0.**

III.5.2 Configuration de protocole HSRP

III.5.2.1 Configuration des SVI (Switch Virtual Interface)

Durant cetteétape,e nous allons configurer les SVI de chaqueVLANn, autrement dit, nous allons attribuer uneadresses IPvirtuellel pour chaqueVLANn sur les deux switches de Core SWC1 et SWC2, cela va nous permettre de faire un routage inter-vlan, mais ce dernier ne se fera pas sauf si on active la fonction de routage avec la commande **ip routing.**

```
SWC1#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
SWC1(config)#IP ROUTING
SWC1(config)#EXIT
SWC1#
%SYS-5-CONFIG_I: Configured from console by console
```

FIGURE III.45 – **Configuration d'ip routing.**

Afin de configurer prochainement le protocole HSRP, à présent nous allons attribuer les adresses aux SVI avec 252 à la partie machines de chaque VLAN sur le SWC1, et sur le SWC2 nous allons faire 253 à la partie machines de chaque VLAN.

```
SWC1(config)#INterface VLan 2
SWC1(config-if)#ip address 10.90.2.252 255.255.255.0
SWC1(config-if)#NO SHutdown
SWC1(config-if)#EXIT
```

FIGURE III.46 – **Configuration SVI sur SWC1.**

Après avoir configuré les SVI de chaqueVLAN,n nous allons vérifier avec la commande **show running-config.**

```
interface Vlan2
 mac-address 0001.43b3.aa01
 ip address 10.90.2.252 255.255.255.0
!
interface Vlan3
 mac-address 0001.43b3.aa02
 ip address 10.90.3.252 255.255.255.0
!
interface Vlan4
 mac-address 0001.43b3.aa03
 ip address 10.90.4.252 255.255.255.0
!
interface Vlan5
 mac-address 0001.43b3.aa04
 ip address 10.90.5.252 255.255.255.0
!
interface Vlan6
 mac-address 0001.43b3.aa05
 ip address 10.90.6.252 255.255.255.0
!
interface Vlan7
 mac-address 0001.43b3.aa06
 ip address 10.90.7.252 255.255.255.0
!
interface Vlan8
 mac-address 0001.43b3.aa07
 ip address 10.90.8.252 255.255.255.0
!
interface Vlan9
 mac-address 0001.43b3.aa08
 ip address 10.90.9.252 255.255.255.0
!
interface Vlan10
 mac-address 0001.43b3.aa09
 ip address 10.90.10.252 255.255.255.0
!
interface Vlan11
 mac-address 0001.43b3.aa0a
 ip address 10.90.11.252 255.255.255.0
!
interface Vlan12
 mac-address 0001.43b3.aa0b
 ip address 10.90.12.252 255.255.255.0
!
```

FIGURE III.47 – **Vérification SVI sur SWC1**

Nous allons procéder la même chose sur SWC2 mais avec un 253 sur la partie machines.

```
SWC2(config)#INterface VLan 2
SWC2(config-if)#IP ADDress 10.90.2.253 255.255.255.0
SWC2(config-if)#NO SHutdown
SWC2(config-if)#EXIT
```

FIGURE III.48 – **Configuration SVI sur SWC2.**

Après avoir configuré les SVI de chaque vlan nous allons vérifier avec la commande **show running-config.**

```
interface Vlan2
 mac-address 0001.43b3.aa01
 ip address 10.90.2.253 255.255.255.0
!
interface Vlan3
 mac-address 0001.43b3.aa02
 ip address 10.90.3.253 255.255.255.0
!
interface Vlan4
 mac-address 0001.43b3.aa03
 ip address 10.90.4.253 255.255.255.0
!
interface Vlan5
 mac-address 0001.43b3.aa04
 ip address 10.90.5.253 255.255.255.0
!
interface Vlan6
 mac-address 0001.43b3.aa05
 ip address 10.90.6.253 255.255.255.0
!
interface Vlan7
 mac-address 0001.43b3.aa06
 ip address 10.90.7.253 255.255.255.0
!
interface Vlan8
 mac-address 0001.43b3.aa07
 ip address 10.90.8.253 255.255.255.0
!
interface Vlan9
 mac-address 0001.43b3.aa08
 ip address 10.90.9.253 255.255.255.0
!
interface Vlan10
 mac-address 0001.43b3.aa09
 ip address 10.90.10.253 255.255.255.0
!
interface Vlan11
 mac-address 0001.43b3.aa0a
 ip address 10.90.11.253 255.255.255.0
!
interface Vlan12
 mac-address 0001.43b3.aa0b
 ip address 10.90.12.253 255.255.255.0
!
```

FIGURE III.49 – **Vérification SVI sur SWC2**

III.5.2.2 Configuration de protocole HSRP

Nous allons maintenant configurer le protocole HSRP sur les deux switches de cœur, SWC1 et SWC2. Sur SWC1, pour chaque interface VLAN, la moitié des VLANs (comme dans la configuration STP) seront configurés avec une priorité HSRP de 150 afin qu'ils soient actifs, tandis que l'autre moitié aura une priorité de 110 pour rester en veille. La configuration sera inversée sur SWC2. De plus, le numéro de groupe HSRP utilisé pour chaque interface VLAN correspondra au numéro du VLAN lui-même.

Sur SWC1 pour les VLANs 2 à 6 :

```
SWC1(config)#interface vlan 2
SWC1(config-if)#STAndby 2  IP 10.90.2.254
SWC1(config-if)#STandby 2 PRIority 150
SWC1(config-if)#STandby 2 PREEmpt
SWC1(config-if)#
```

FIGURE III.50 – **Configuration du HSRP (VLAN 2 à 6).**

Sur SWC1 pour les VLANs 7 à 12 :

```
SWC1(config)#interface vlan 7
SWC1(config-if)#STandby 7 IP 10.90.7.254
SWC1(config-if)#STandby 7 PRIority 110
SWC1(config-if)#STandby 7 PREEmpt
SWC1(config-if)#EXIT
```

FIGURE III.51 – **Configuration du HSRP (VLAN 7 à 12).**

On procédera de même pour le SWC2 :
Sur SWC2 pour les VLANs 2 à 6 :

```
SWC2(config)#interface vlan 2
SWC2(config-if)#STandby 2 IP 10.90.2.254
SWC2(config-if)#STandby 2 PRIOrity 110
SWC2(config-if)#STandby 2 PREEmpt
SWC2(config-if)#
```

FIGURE III.52 – **Configuration du HSRP (VLAN 2 à 6).**

Sur SWC2 pour les VLANs 7 à 12 :

```
SWC2(config)#interface vlan 7
SWC2(config-if)#STandby 7 IP 10.90.7.254
SWC2(config-if)#STandby 7 PRIority 150
SWC2(config-if)#STandby 7 PREEmpt
```

FIGURE III.53 – **Configuration du HSRP (Vlan 7 à 12).**

Nous allons vérifier cette configuration avec la commande **show standby brief**.
Sur SWC1 :

```
SWC1#SHow STANdby BRief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
V12         2    150 P Active   local           10.90.2.254     10.90.2.254
V13         3    150 P Active   local           10.90.3.253     10.90.3.254
V14         4    150 P Active   local           10.90.4.253     10.90.4.254
V15         5    150 P Active   local           10.90.5.253     10.90.5.254
V16         6    150 P Active   local           10.90.6.253     10.90.6.254
V17         7    110 P Standby  10.90.7.253     local           10.90.7.254
V18         8    110 P Standby  10.90.8.253     local           10.90.8.254
V19         9    110 P Standby  10.90.9.253     local           10.90.9.254
V110        10   110 P Standby  10.90.10.253    local           10.90.10.254
V111        11   110 P Standby  10.90.11.253    local           10.90.11.254
V112        12   110 P Standby  10.90.12.253    local           10.90.12.254
```

FIGURE III.54 – **Vérification du HSRP sur SWC1.**

Sur SWC2 :

```
SWC2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
V12         2    110 P Standby  10.90.2.252     local           10.90.2.254
V13         3    110 P Standby  10.90.3.252     local           10.90.3.254
V14         4    110 P Standby  10.90.4.252     local           10.90.4.254
V15         5    110 P Standby  10.90.5.252     local           10.90.5.254
V16         6    110 P Standby  10.90.6.252     local           10.90.6.254
V17         7    150 P Active   local           10.90.7.252     10.90.7.254
V18         8    150 P Active   local           10.90.8.252     10.90.8.254
V19         9    150 P Active   local           10.90.9.252     10.90.9.254
V110        10   150 P Active   local           10.90.10.252    10.90.10.254
V111        11   150 P Active   local           10.90.11.252    10.90.11.254
V112        12   150 P Active   local           10.90.12.252    10.90.12.254
```

FIGURE III.55 – **Vérification du HSRP sur SWC2.**

III.5.2.3 Configurations de Protocole OSPF :

Ici pour l'OSPF, nous allons configurer ce protocole au niveau des switches du Core.Nous allons tout d'abord convertir les ports de niveau 2 au niveau 3 et les faire fonctionner comme des interfaces de routeur en utilisant la commande « **no switchport** », puis on attribue une adresse **IP/30** et un masque de réseau pour chacun des ports routés. Les figures ci-dessous montrent la configuration des ports routés :

Sur le SWC1 :

```
SWC1(config-if)#interface gigabitEthernet 1/0/1
SWC1(config-if)#NO SWitchport
SWC1(config-if)#IP ADDress 172.31.16.2 255.255.255.252
SWC1(config-if)#NO SHutdown
SWC1(config-if)#EXIT
```

FIGURE III.56 – **Configuration des ports routés sur SWC1.**

Sur le SWC1 :

```
SWC1(config)#interface gigabitEthernet 1/0/1
SWC1(config-if)#NO SWitchport
SWC1(config-if)#IP ADDress 172.32.1.2 255.255.255.252
SWC1(config-if)#NO SHutdown
SWC1(config-if)#EXIT
```

FIGURE III.57 – **Configuration des ports routés sur SWC2.**

Sur le routeur Router R1 :

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#IP ADDress 172.31.16.1 255.255.255.252
R1(config-if)#NO SH
R1(config-if)#interface gigabitEthernet 0/1
R1(config-if)#IP ADDress 172.32.1.1 255.255.255.252
R1(config-if)#NO SH
```

FIGURE III.58 – **Configuration des ports routés sur R1.**

Ensuite, nous allons activer le routage OSPF en utilisant le processus numéro 1. Sur chaque switch, nous déclarerons l'ensemble des réseaux directement connectés. Pour les VLANs, nous spécifierons le réseau 10.90.0.0 avec un masque inversé de 0.0.0.255. comme suit :

Sur SWC1 :

```
SWC1#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
SWC1(config)#IP ROUTING
SWC1(config)#router ospf 1
SWC1(config-router)#NETWORK 172.31.16.0 0.0.0.3 area 0
SWC1(config-router)#NETWORK 10.90.2.0 0.0.0.255 area 0
SWC1(config-router)#NETWORK 10.90.3.0 0.0.0.255 area 0
SWC1(config-router)#NETWORK 10.90.4.0 0.0.0.255 area 0
SWC1(config-router)#NETWORK 10.90.5.0 0.0.0.255 area 0
SWC1(config-router)#NETWORK 10.90.6.0 0.0.0.255 area 0
SWC1(config-router)#NETWORK 10.90.7.0 0.0.0.255 area 0
SWC1(config-router)#NETWORK 10.90.8.0 0.0.0.255 area 0
SWC1(config-router)#NETWORK 10.90.9.0 0.0.0.255 area 0
SWC1(config-router)#NETWORK 10.90.10.0 0.0.0.255 area 0
SWC1(config-router)#NETWORK 10.90.11.0 0.0.0.255 area 0
SWC1(config-router)#NETWORK 10.90.12.0 0.0.0.255 area 0
SWC1(config-router)#EXIT
```

FIGURE III.59 – **Configuration de l'OSPF sur SWC1.**

Sur SWC2 :

```
SWC2(config)#IP ROUTING
SWC2(config)#ROUTER OSPF 1
SWC2(config-router)#NETWORK 10.90.2.0 0.0.0.255 area 0
SWC2(config-router)#NETWORK 10.90.3.0 0.0.0.255 area 0
SWC2(config-router)#NETWORK 10.90.4.0 0.0.0.255 area 0
SWC2(config-router)#NETWORK 10.90.5.0 0.0.0.255 area 0
SWC2(config-router)#NETWORK 10.90.6.0 0.0.0.255 area 0
SWC2(config-router)#NETWORK 10.90.7.0 0.0.0.255 area 0
SWC2(config-router)#NETWORK 10.90.8.0 0.0.0.255 area 0
SWC2(config-router)#NETWORK 10.90.9.0 0.0.0.255 area 0
SWC2(config-router)#NETWORK 10.90.10.0 0.0.0.255 area 0
SWC2(config-router)#NETWORK 10.90.11.0 0.0.0.255 area 0
SWC2(config-router)#NETWORK 10.90.12.0 0.0.0.255 area 0
SWC2(config-router)#NETWORK 172.32.1.0 0.0.0.3 area 0
SWC2(config-router)#EXIT
```

FIGURE III.60 – **Configuration de l'OSPF sur SWC2.**

Sur R1 :

```
R1(config)#IP ROUTING
R1(config)#ROUTER OSPF 1
R1(config-router)#NETWORK 172.31.16.0 0.0.0.3 area 0
R1(config-router)#NETWORK 172.32.1.0 0.0.0.3 area 0
R1(config-router)#END
```

FIGURE III.61 – **Configuration de l'OSPF sur R1.**

Et nous pouvons vérifier avec la commande **Show IP route**

```
R1#SH IP ROUTE
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 11 subnets
O       10.90.2.0/24 [110/2] via 172.32.1.2, 00:02:00, GigabitEthernet0/1
O       10.90.3.0/24 [110/2] via 172.32.1.2, 00:02:00, GigabitEthernet0/1
O       10.90.4.0/24 [110/2] via 172.32.1.2, 00:02:00, GigabitEthernet0/1
O       10.90.5.0/24 [110/2] via 172.32.1.2, 00:02:00, GigabitEthernet0/1
O       10.90.6.0/24 [110/2] via 172.32.1.2, 00:02:00, GigabitEthernet0/1
O       10.90.7.0/24 [110/2] via 172.32.1.2, 00:02:00, GigabitEthernet0/1
O       10.90.8.0/24 [110/2] via 172.32.1.2, 00:02:00, GigabitEthernet0/1
O       10.90.9.0/24 [110/2] via 172.32.1.2, 00:02:00, GigabitEthernet0/1
O       10.90.10.0/24 [110/2] via 172.32.1.2, 00:02:00, GigabitEthernet0/1
O       10.90.11.0/24 [110/2] via 172.32.1.2, 00:02:00, GigabitEthernet0/1
O       10.90.12.0/24 [110/2] via 172.32.1.2, 00:02:00, GigabitEthernet0/1
     172.31.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.31.16.0/30 is directly connected, GigabitEthernet0/0
L       172.31.16.1/32 is directly connected, GigabitEthernet0/0
     172.32.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.32.1.0/30 is directly connected, GigabitEthernet0/1
L       172.32.1.1/32 is directly connected, GigabitEthernet0/1
```

FIGURE III.62 – **Vérification de l'OSPF.**

III.5.2.4 Test de la haute disponibilité du réseau

Afin de tester le bon fonctionnement de notre réseau LAN et de s'assurer qu'il est opérationnel, nous allons simuler un ping continu entre deux PCs du même VLAN, puis nous allons simuler une panne sur leur switch Root Bridge en éteignant les ports de ce dernier, et on vérifie que le ping

III.5.2.4.1 Test de haute disponibilité entre Pcs : Premièrement, nous avons pris un PC du VLA 2 (10.90.2.1) et nous allons faire un Ping continu vers un PC du VLAN (10.90.5.2), En premier lieu nous avons constaté que le Ping fonctionne parfaitement et sans problème,

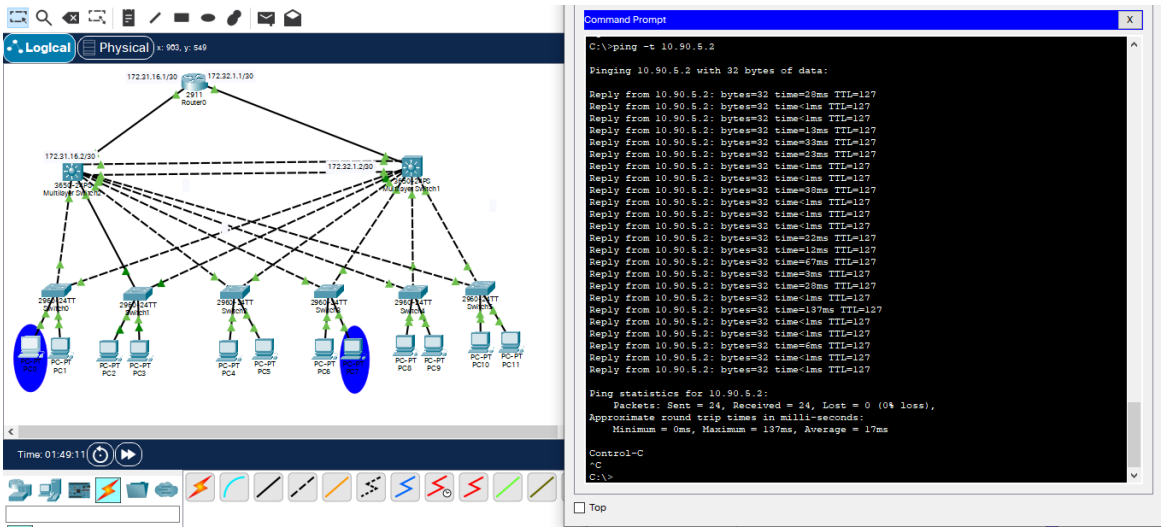

FIGURE III.63 – **Ping continu entre deux PC.**

Maintenant nous visons à simuler une panne de la route principale du VLAN 2 et nous allons constater directement que le ping s'arrête, Juste après 5 ou 6 arrêts le protocole HSRP discute avec le SWC2 et active automatiquement la route qui est en standby. Nous allons constater directement que le ping reprend, ce qui prouve que la route a bien été basculée vers le SWC2.

comme est :

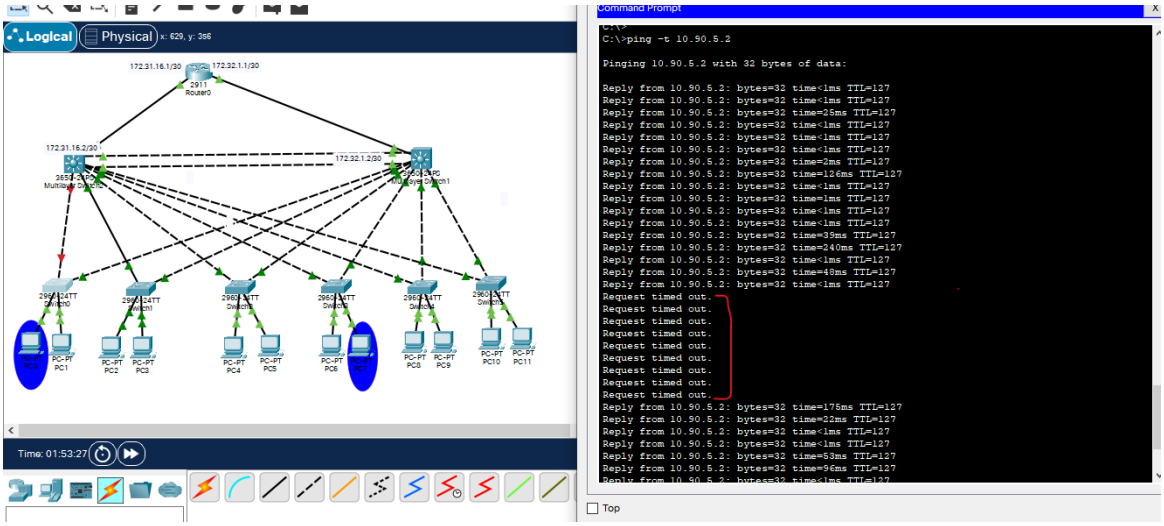

FIGURE III.64 – **Ping continu lors d'une panne de la route principale de VLAN 2**

Maintenant, nous allons réactiver l'interface principale sur le SWC1 afin de s'assurer qu'il va reprendre sa route principale et vérifier que le preempt du HSRP fonctionne parfaitement. Dès qu'on active l'interface, on constate qu'il y a encore un arrêt dans le Ping, le temps que les deux switches discutent les priorités puis il reprend facilement sa route et le Ping remarche.

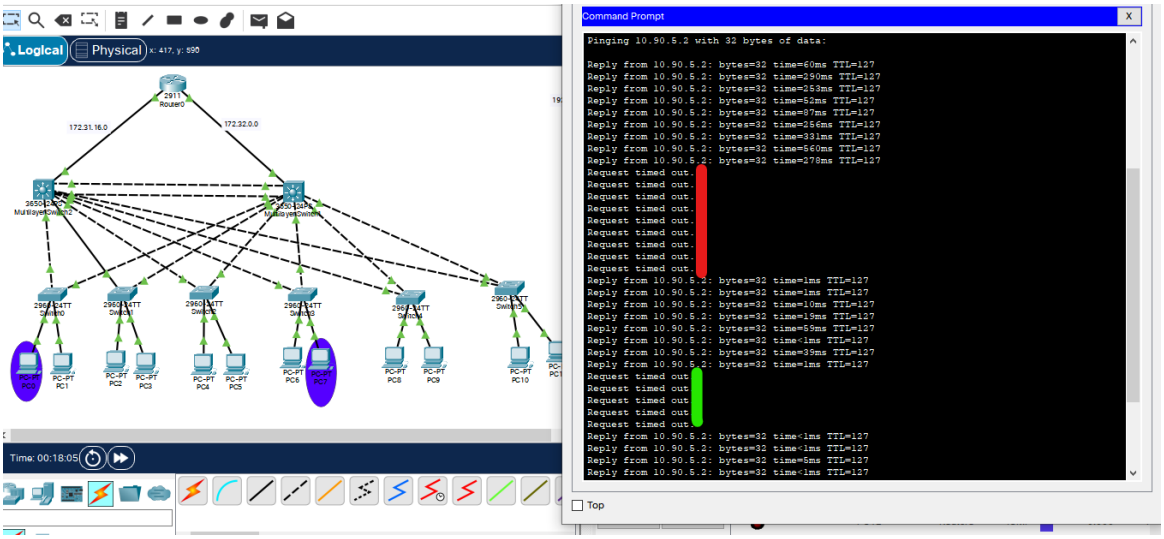

FIGURE III.65 – **Réactivation de la route principale du VLAN 2**

III.5.2.4.2 Test de la haute disponibilité du réseau LAN : Suivant la même méthode, nous allons tester la haute disponibilité de tout le réseau local de Cevital,

en simulant une défaillance de l'un des switches de Core (SWC1) Sur un PC du VLAN2 (10.90.2.1), nous allons réaliser un Ping continu vers Vlan 6 (10.90.6.5).

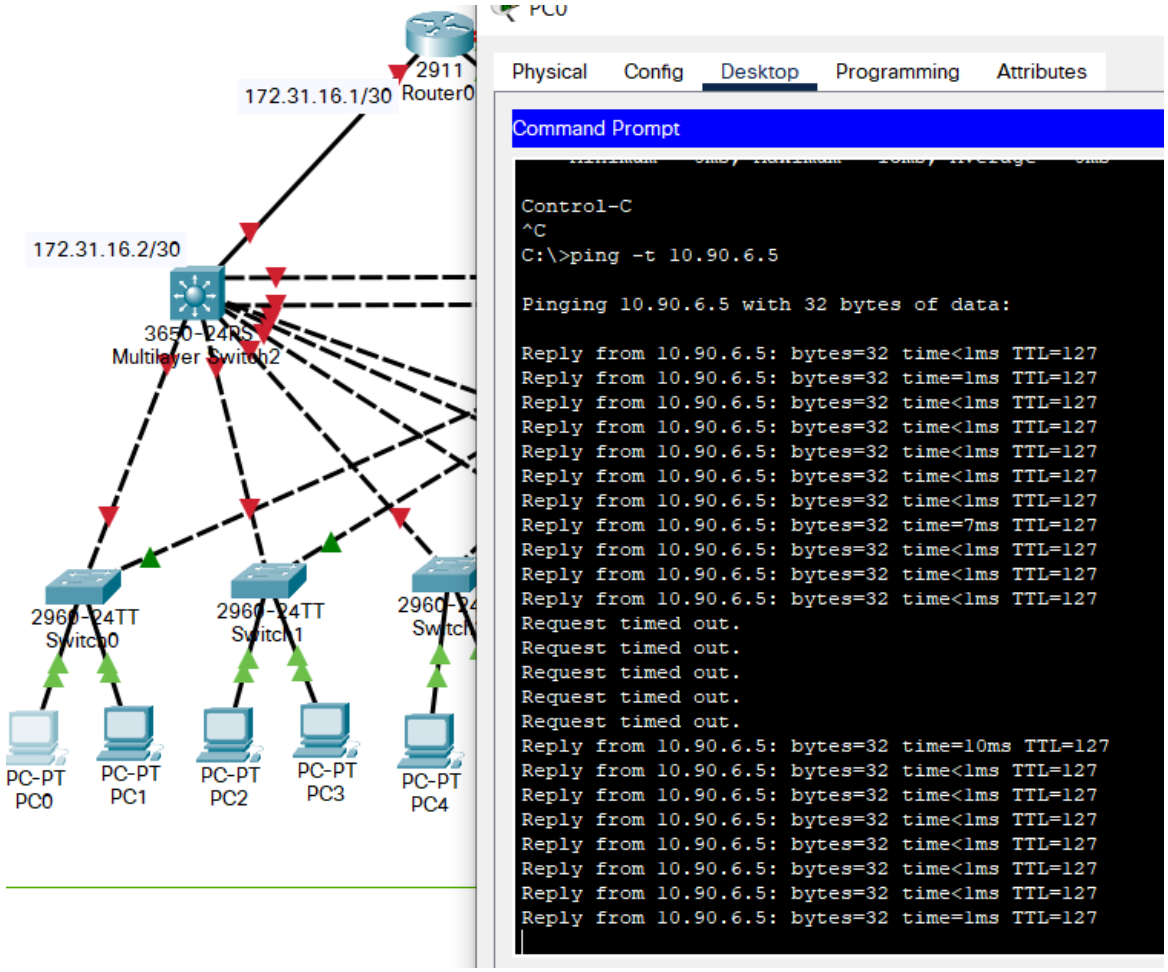

FIGURE III.66 – **Simulation d'une panne sur SWC1 et impact sur la connectivité.**

La simulation de la panne a provoqué une interruption temporaire du ping. Le switch SWC2, ayant la deuxième priorité HSRP la plus élevée, a pris le relais en tant que switch principal du VLAN 2. Le processus de basculement a entraîné une perte de 5 à 6 paquets pendant la période nécessaire pour que le switch standby prenne le relais.

— **Réactivation du switch principal et test de la préemption HSRP :**

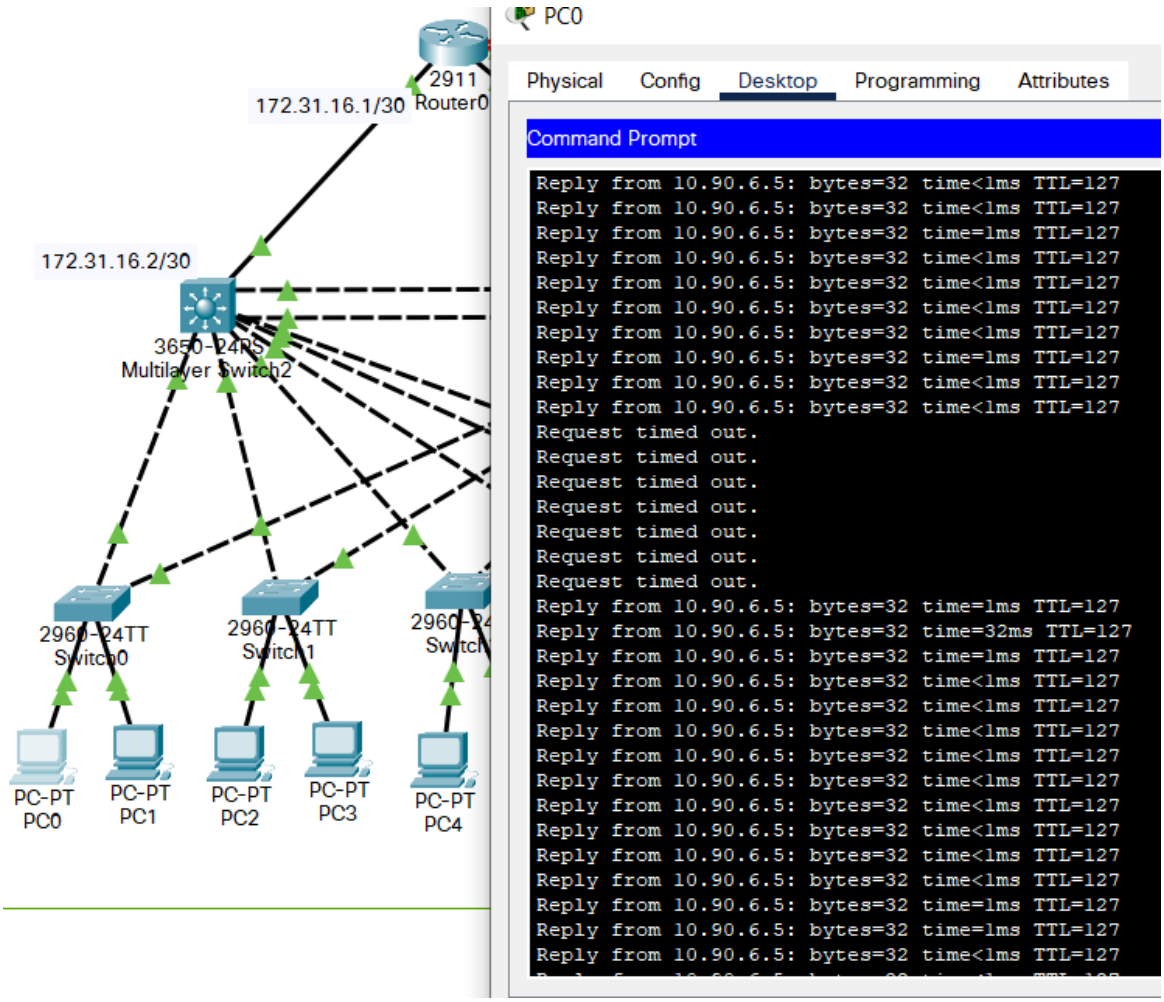

FIGURE III.67 – **Réactivation du switch principale**

Le test a été réalisé avec succès. Quand le switch principal a été remis en service, une interruption temporaire du ping a été observée, mais le HSRP a rapidement effectué la préemption et SWC1 est redevenu le switch principal du VLAN 2. Le ping a ensuite repris sans interruption.

III.6 La mise en place d'un réseau WAN redondant

III.6.1 Architecture WAN

Nous avons configuré la nouvelle architecture proposée au réseau Cevital sur le simulateur CISCO Packet Tracer 8.1.1 La topologie est représentée ci-dessous.

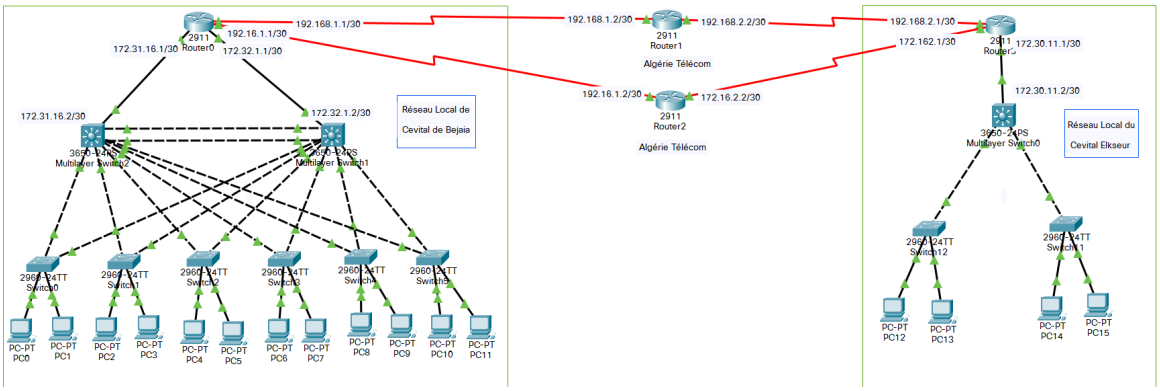

FIGURE III.68 – **Architecture WAN de Cevital.**

III.6.2 Configuration des équipements du réseau WAN

Dans cette partie, nous avons interconnecté le réseau local de la première partie au site distant d'EL Kseur avec des liaisons spécialisées (une liaison fibre optique entre le site distant et le site de Béjaïa via Algérie Telecom et une liaison (FH) entre le site distant et le site de Béjaïa via Algérie Telecom) afin de permettre le partage de ressources et de la communication.

— **Configuration LAN :** nous avons conservé la même architecture LAN ainsi que les configurations de la première partie du chapitre, en y ajoutant toutefois les interfaces montantes du Routeur 1, respectivement vers les routeurs d'Algérie Télécom et vers le switch cœur.

— **Configuration WAN :** Pour garantir le routage du réseau, nous avons configuré le protocole OSPF au niveau des routeurs qui relient le site distant. Nous avons attribué le processus OSPF numéro 1 et défini les aires dans chaque configuration, en déclarant les réseaux directement connectés sur chaque routeur.

III.6.2.1 VLANs utilisés dans la topologie WAN

Direction	VLAN	DHCP	Root	IP SWC	Passerelle
Commercial	VLAN 13	Dynamique	SWC	10.30.13.254	10.30.13.254
Marketing	VLAN 14	Dynamique	SWC	10.30.14.254	10.30.14.254
Cevital-Wifi	VLAN 15	Dynamique	SWC	10.30.15.254	10.30.14.254
Control-Acces	VLAN 16	Dynamique	SWC	10.30.16.254	10.30.13.254

III.6.2.2 Tableaux des interfaces

tableau d'attribution des adresses IP pour les interfaces des routeurs

Routeur	Interfaces (Adresse IP)
Routeur0	Se0/2/0 : 192.168.1.1/30
	Se0/2/1 : 192.16.1.1/30
	Gig0/0 : 172.31.16.1/30
	Gig0/1 : 172.32.1.1/30
Routeur1	Se0/2/0 : 192.168.1.2/30
	Se0/2/1 : 192.168.2.2/30
Routeur2	Se0/2/1 : 192.16.1.2/30
	Se0/3/0 : 172.16.2.2/30
Routeur3	Se0/3/0 : 192.168.2.1/30
	Se0/3/1 : 172.16.2.1/30
	Gig0/0 : 172.30.11.1/30

TABLE III.5 – **Attribution des adresses IP pour les interfaces des routeurs**

Tableau d'attribution des adresses IP pour les interfaces des switchs

En utilisant la commande « no switchport », puis on attribue une adresse IP/30

switch	Interfaces (Adresse IP)
switch ELKSEUR	Gig1/0/3 : 172.30.11.2/30
SWC1 Cevital	Gig1/0/1 : 172.31.16.2/30
SWC2 Cevital	Gig1/0/1 : 172.32.1.2/30

TABLE III.6 – **Attribution des adresses IP pour les interfaces des switchs**

III.6.2.3 Configuration des interfaces

Avant de configurer le routage OSPF, nous allons d'abord configurer les interfaces avec des adresses IP comme indiquées sur Tableau .

Exemple sur R1 :

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#in
R1(config)#interface se0/2/0
R1(config-if)#IP ADD 192.168.1.1 255.255.255.252
R1(config-if)#NO SH

R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/0, changed state to up

R1(config-if)#interface se0/2/1
R1(config-if)#IP ADD 192.16.1.1 255.255.255.252
R1(config-if)#NO SH
R1(config-if)#EXIT
R1(config)#interface gig0/0
R1(config-if)#IP ADD 172.31.16.1 255.255.255.252
R1(config-if)#NO SH
R1(config-if)#EXIT
R1(config)#INTERFACE GIG0/1
R1(config-if)#IP ADD 172.32.1.1 255.255.255.252
R1(config-if)#NO SH
R1(config-if)#
```

FIGURE III.69 – **Configuration des interfaces du R1**

Vérification des interfaces

Avec la commande « **show running-config** »

```
!
interface GigabitEthernet0/0
 ip address 172.31.16.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.32.1.1 255.255.255.252
 duplex auto
 speed auto
!
```

```
interface Serial0/2/0
 ip address 192.168.1.1 255.255.255.252
 clock rate 2000000
!
interface Serial0/2/1
 ip address 192.16.1.1 255.255.255.252
 clock rate 2000000
!
```

FIGURE III.70 – **Vérification des interfaces de R1**

La même configuration sera réalisée sur les différents routeurs ET switches en respectant les tableaux.

III.6.2.4 Configuration de l'OSPF

Nous avons alloué le même groupe OSPF1 sur tous les routeurs et switches, et attribué les memes aires pour chacun.

Sur routeur de Cevital Bejaia

```
R1(config)#ROUTER OSPF 1
R1(config-router)#NETWORK 172.31.16.1 0.0.0.3 area 0
R1(config-router)#network 172.32.1.1 0.0.0.3 area 0
R1(config-router)#network 192.16.1.1 0.0.0.3 area 0
R1(config-router)#network 192.168.1.1 0.0.0.3 area 0
R1(config-router)#EXIT
```

FIGURE III.71 – **Configuration de l'OSPF sur routeur Bejaia.**

Sur routeur 1 Algerie Telecom Bejaia

```
ROUTER1(config)#IP ROUTING
ROUTER1(config)#router ospf 1
ROUTER1(config-router)#network 192.168.1.2 0.0.0.3 area 0
ROUTER1(config-router)#network 192.168.2.2 0.0.0.3 area 0
ROUTER1(config-router)#EXIT
```

FIGURE III.72 – **configuration de l'OSPF sur routeur Algerie telecom de bejaia.**

Sur routeur 2 Algerie Telecom ElKseur

```
router2(config)#IP ROUTING
router2(config)#router ospf 1
router2(config-router)#NETwork 192.168.1.2 0.0.0.3 area 0
router2(config-router)#network 172.16.2.2 0.0.0.3 area 0
router2(config-router)#EXIT
```

FIGURE III.73 – **configuration de l'OSPF sur routeur Algerie Telecom ElKseur .**

Sur routeur de Cevital ElKseur

```
ELKSEUR(config)#IP ROUTING
ELKSEUR(config)#router ospf 1
ELKSEUR(config-router)#network 192.168.2.1 0.0.0.3 area 0
ELKSEUR(config-router)#network 172.16.2.1 0.0.0.3 area 0
ELKSEUR(config-router)#network 172.30.11.1 0.0.0.3 area 0
ELKSEUR(config-router)#EXIT
```

FIGURE III.74 – **configuration de l'OSPF sur routeur Cevital ElKseur .**

Vérification de l'OSPF Avec la commande « **show running-config** ». **sur les routeurs**

```
router ospf 1
 no log-adjacency-changes
 network 192.168.1.0 0.0.0.3 area 0
 network 192.16.1.0 0.0.0.3 area 0
 network 172.32.0.0 0.0.0.3 area 0
 network 172.31.16.0 0.0.0.3 area 0
 network 172.32.1.0 0.0.0.3 area 0
!
```

```
router ospf 1
 log-adjacency-changes
 network 172.30.11.0 0.0.0.3 area 0
 network 192.168.2.0 0.0.0.3 area 0
 network 172.16.2.0 0.0.0.3 area 0
!
```

FIGURE III.75 – **Vérification de l'OSPF sur routeur Cevital de Bejaia et routeur Cevital ElKseur.**

sur le switch de site distant

```
router ospf 1
 log-adjacency-changes
 network 10.30.0.0 0.0.0.255 area 0
 network 172.30.11.0 0.0.0.3 area 0
 network 10.30.13.0 0.0.0.255 area 0
 network 10.30.14.0 0.0.0.255 area 0
 network 10.30.15.0 0.0.0.255 area 0
 network 10.30.16.0 0.0.0.255 area 0
!
```

FIGURE III.76 – **Vérification de configuration de l'OSPF sur le site distant**

III.6.2.5 Test de connectivité WAN

Nous allons vérifier que la connexion inter-sites est opérationnelle, pour ce faire nous allons simuler un Ping entre un PC du site local (Bejaia) vers un PC du site distant(ElKseur).

La commande « **Ping –t** » nous permet de simuler un Ping continu, et « **tracert** » permet de suivre le chemin des paquets qui transitent de la source vers la destination.

Sur la figure suivant, on remarque que les paquets transitent du PC0 (10.90.2.1) du site local vers le PC du site distant (10.30.13.1) à partir de la route principale 1 (192.168.1.2)

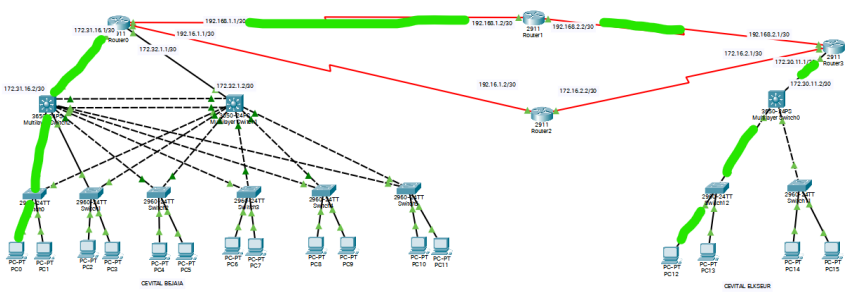

FIGURE III.77 – **le ping du pc local au PC distant**

```
C:\>ping -t 10.30.13.1

Pinging 10.30.13.1 with 32 bytes of data:

Reply from 10.30.13.1: bytes=32 time=2ms TTL=123
Reply from 10.30.13.1: bytes=32 time=2ms TTL=123
Reply from 10.30.13.1: bytes=32 time=11ms TTL=123
Reply from 10.30.13.1: bytes=32 time=10ms TTL=123
Reply from 10.30.13.1: bytes=32 time=2ms TTL=123
Reply from 10.30.13.1: bytes=32 time=2ms TTL=123
Reply from 10.30.13.1: bytes=32 time=3ms TTL=123
Reply from 10.30.13.1: bytes=32 time=3ms TTL=123
Reply from 10.30.13.1: bytes=32 time=10ms TTL=123

Ping statistics for 10.30.13.1:
    Packets: Sent = 9, Received = 9, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 11ms, Average = 5ms
```

FIGURE III.78 – **verification du ping du pc local au PC distant.**

```
C:\>tracert 10.30.13.1

Tracing route to 10.30.13.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      10.90.2.252
  2    11 ms     0 ms      7 ms      172.31.16.1
  3    10 ms     1 ms      0 ms      192.168.1.2
  4    10 ms     1 ms      1 ms      192.168.2.1
  5    2 ms      0 ms      1 ms      172.30.11.2
  6    10 ms     10 ms     14 ms     10.30.13.1

Trace complete.
```

FIGURE III.79 – **verification du traceroute du route principale.**

Maintenant nous allons simuler une panne, celle d'éteindre la route principale.Nous allons constater directement que le Ping s'arrête pour quelques paquets pour activer la route secondaire de l'adresse IP(192.16.1.2), puis le Ping reprend, ce qui prouve que la route a bien été basculée.

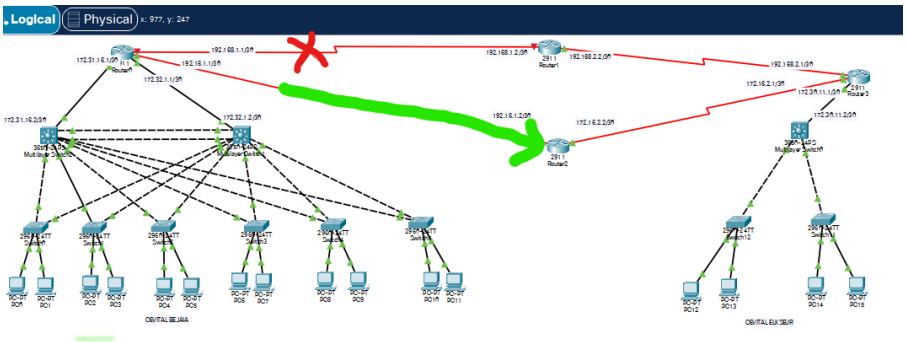

FIGURE III.80 – **Blokage de la route pricipale 1.**

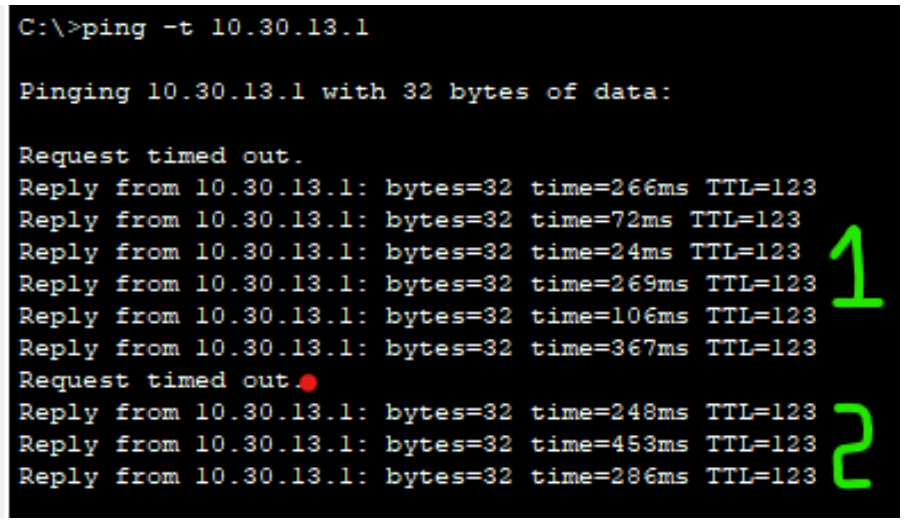

FIGURE III.81 – **verificationdu ping du route secondaire 2. vers le pc du site distant**

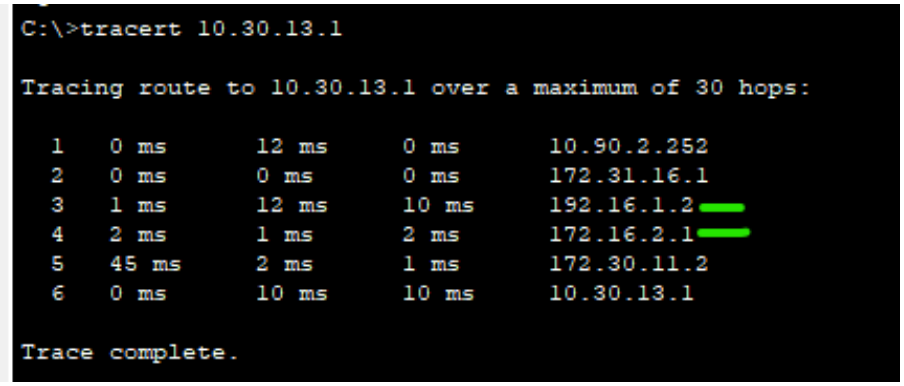

FIGURE III.82 – **verification du traceroute du route secondaire .**

III.7 Conclusion :

Ce chapitre s'est scindé en deux parties. Dans la première, nous avons configuré le réseau LAN proposé, où nous avons mis les configurations et les protocoles de redondance, à savoir la configuration des VLANs, des liens Trunk, les protocoles VTP, HSRP, etc. Puis dans la deuxième nous avons mis en place des connexions redondantes vers les sites distants du Cevital, en utilisant le protocole de routage OSPF. Les résultats obtenus et détaillés dans ce chapitre démontrent que le réseau proposé est la solution adéquate à la problématique.

Conclusion Générale

La haute disponibilité est aujourd'hui un enjeu majeur pour toute entreprise, quel que soit son secteur ou sa taille. Un réseau fiable et constamment opérationnel permet de prévenir des pertes importantes de productivité, de ressources et de dépenses associées aux interruptions de service.

Ce mémoire nous a permis d'étudier en profondeur le réseau LAN/WAN du complexe Cevital à Béjaïa, d'appliquer nos connaissances théoriques acquises, et de mieux analyser son fonctionnement durant notre période de stage. Le thème de la haute disponibilité, centré sur le protocole HSRP, nous a amenés à identifier les faiblesses du système existant et à proposer une infrastructure plus résiliente, basée sur la redondance matérielle et logicielle.

Pour garantir la redondance et la continuité de service, un second switch (SWC2) a été ajouté en complément de SWC1, avec une répartition de charge et une liaison EtherChannel entre eux pour un débit élevé. Au niveau de la couche cœur, plusieurs protocoles ont été configurés : SSH pour un accès sécurisé, STP pour éviter les boucles, avec un partage des rôles de root bridge entre SWC1 et SWC2 pour équilibrer le trafic. La gestion des VLANs est assurée via VTP, et la haute disponibilité par le protocole HSRP. Enfin, le routage dynamique est assuré par OSPF, déployé sur les switches du cœur et le routeur. Les tests et les simulations ont été réalisés via Cisco Packet Tracer 8.1.1, un outil simple et efficace pour ce type d'architecture.

Cette expérience nous a offert une opportunité précieuse de découvrir un environnement informatique industriel vaste et complexe, tout en consolidant nos compétences techniques liées à la continuité de service 24h/24.

En conclusion, ce mémoire confirme la pertinence de l'utilisation du HSRP pour renforcer la résilience des réseaux industriels, et constitue une base solide pour des travaux ultérieurs en amélioration des performances réseaux.

Annexes

.1 présentation du simulateur cisco parcket tracer

Cisco Packet Tracer est un simulateur de matériel réseaux permettant de créer et tester des réseaux virtuels. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, commutateurs et ordinateurs, reliés par différents types de câbles. Une fois connectés, ces appareils peuvent être configurés (adresses IP, services réseau, etc.) pour simuler le fonctionnement réel d'un réseau. L'outil permet aussi de visualiser le trajet des paquets et d'analyser le comportement des protocoles, ce qui en fait un excellent support pour l'apprentissage des réseaux.

.2 Description générale

La figure 1 montre un aperçu général de Packet Tracer. La zone (1) est la partie dans laquelle le réseau est construit. Les équipements sont regroupés en catégories accessibles dans la zone (2). Une fois la catégorie sélectionnée, le type d'équipement peut être sélectionné dans la zone (3). La zone (6) contient un ensemble d'outils :

— Select : pour déplacer ou éditer des équipements.

— Move Layout : permet de déplacer le plan de travail.

— Place Note : place des notes sur le réseau.

— Delete : supprime un équipement ou une note.

— Inspect : permet d'ouvrir une fenêtre d'inspection sur un équipement (tableARP, routage). La zone (5) permet d'ajouter des indications dans le réseau. Enfin, la zone (4) permet de passer du mode temps réel au mode simulation.

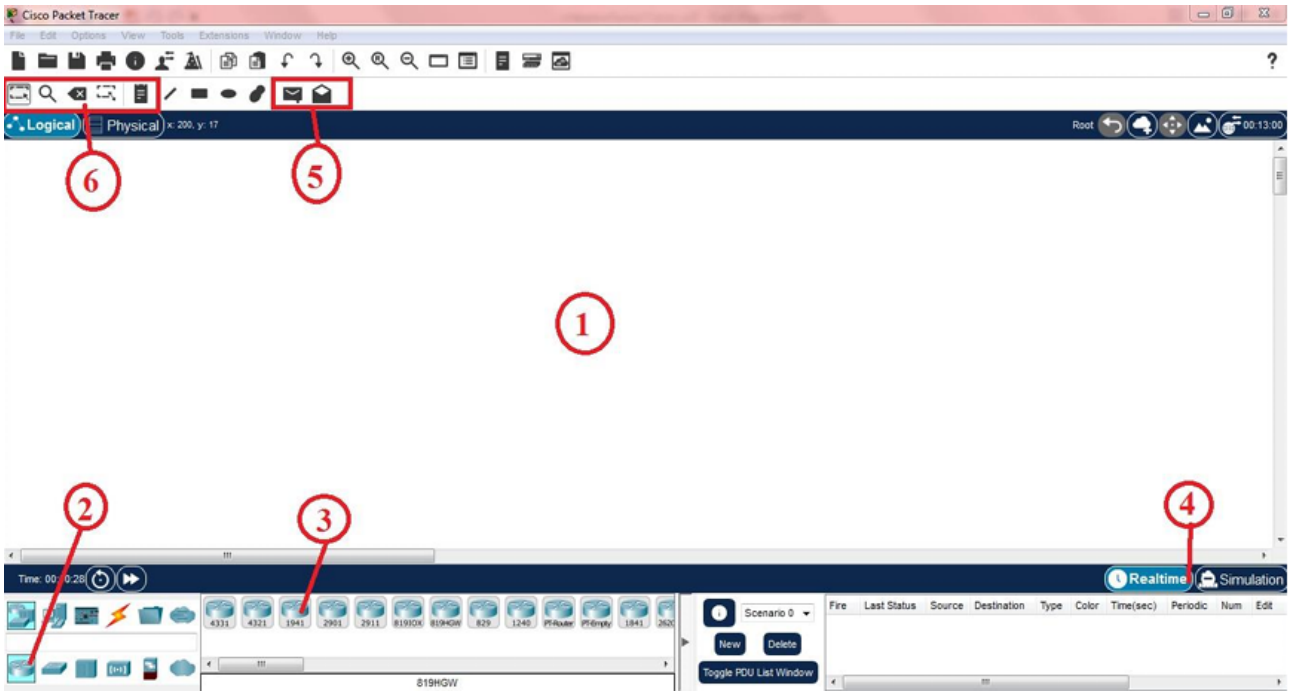

FIGURE 83 – **environnement de Cisco Packet Tracer.**

.3 Ajout d'un équipement

Pour ajouter un équipement l'utilisateur doit sélectionner un type d'équipement parmi les catégories proposées par ce simulateur y'on trouve : les routeurs, les commutateurs, les hubs, les équipements sans-fil, les connexions, les équipements dit terminaux (ordinateur, serveur), des équipements personnalisées et connexion multiutilisateur. Lorsqu'une catégorie est sélectionnée l'utilisateur a le choix entre plusieurs équipements différents .il suffit donc de cliquer dessus puis de cliquer à l'endroit choisi et en fin cliquer sur l'espace de travail.

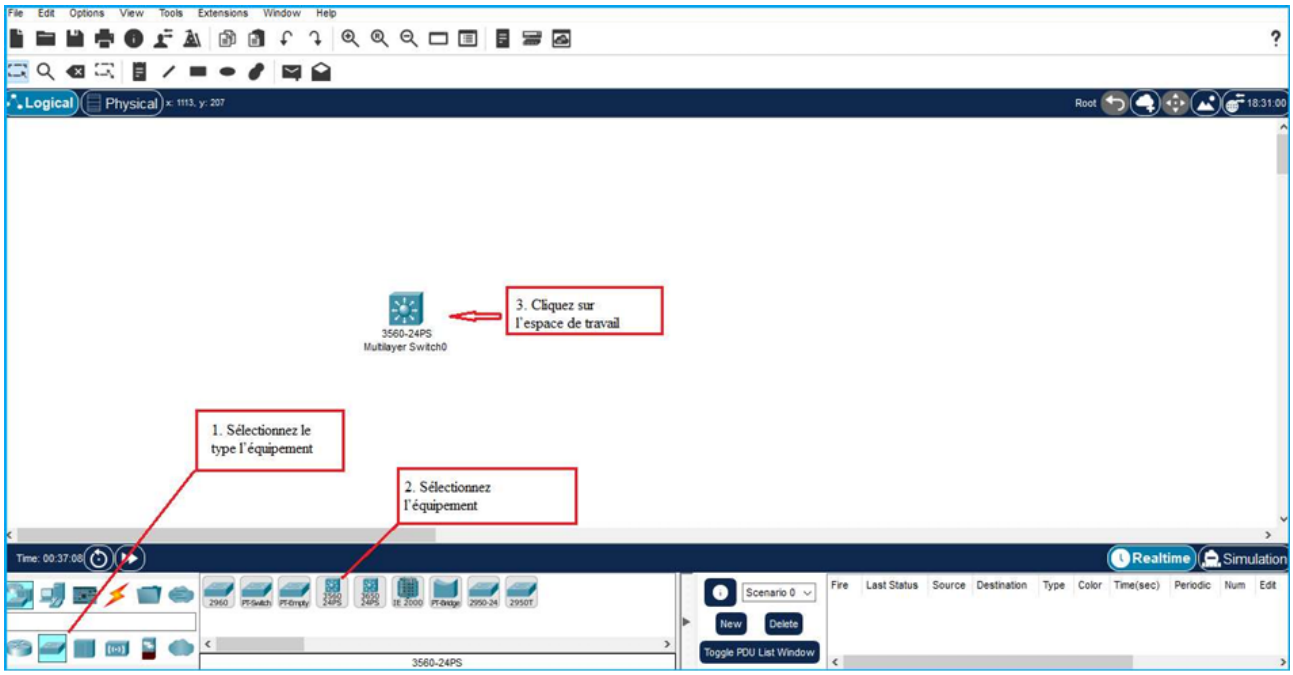

FIGURE 84 – **Capture d'ajout d'un équipement .**

.4 Création d'une connexion

Pour relier deux équipements il faut choisir la catégorie connexion et cliquer sur la connexion souhaitée, puis choisir l'interface désirée sur le premier équipement et enfin cliquer sur le deuxième équipement et choisir l'interface désirée aussi. La connexion est visible sur la capture suivante :

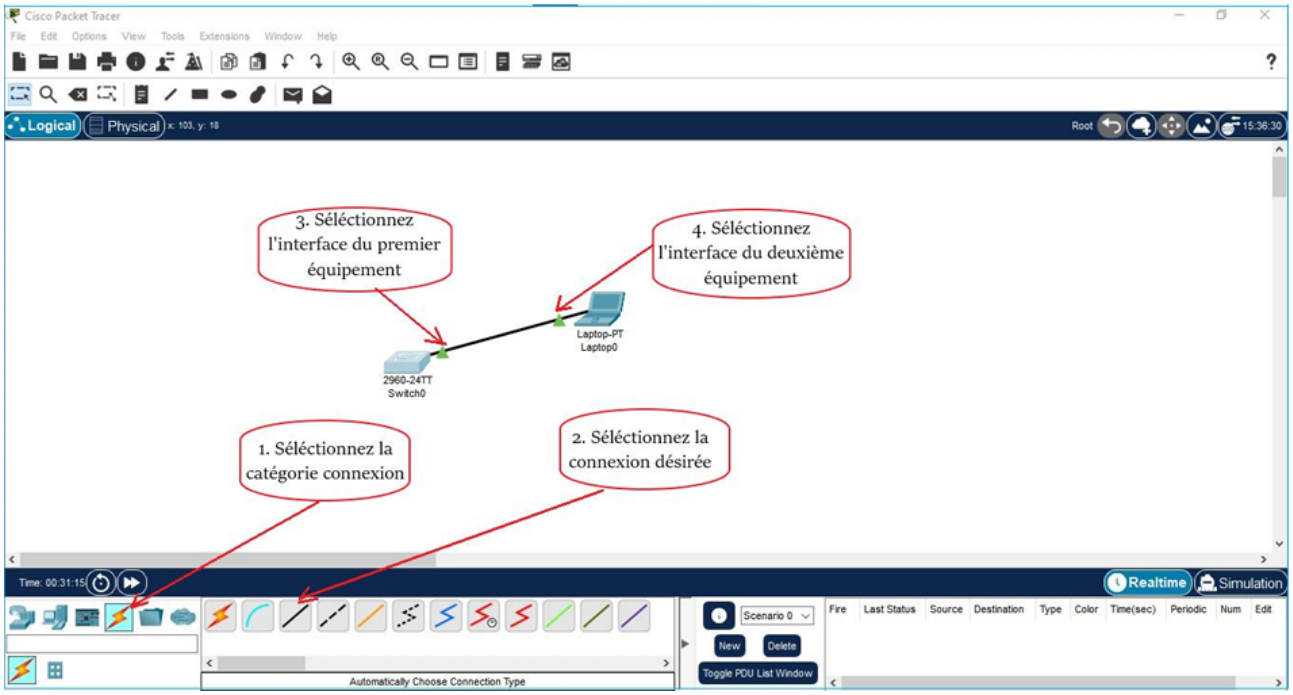

FIGURE 85 – **Capture création d'une connexion entre deux équipements .**

.5 Configuration d'un équipement

Lorsqu'un équipement est ajouté, il est possible de le configurer en cliquant dessus, une fois ajouté dans le réseau. Une nouvelle fenêtre s'ouvre comportant différents onglets : Physical, config, desktop, CLI & etc. Généralement pour les ordinateurs on utilise l'onglet config pour configurer l'adresse IP et le DNS et tout le nécessaire du PC.

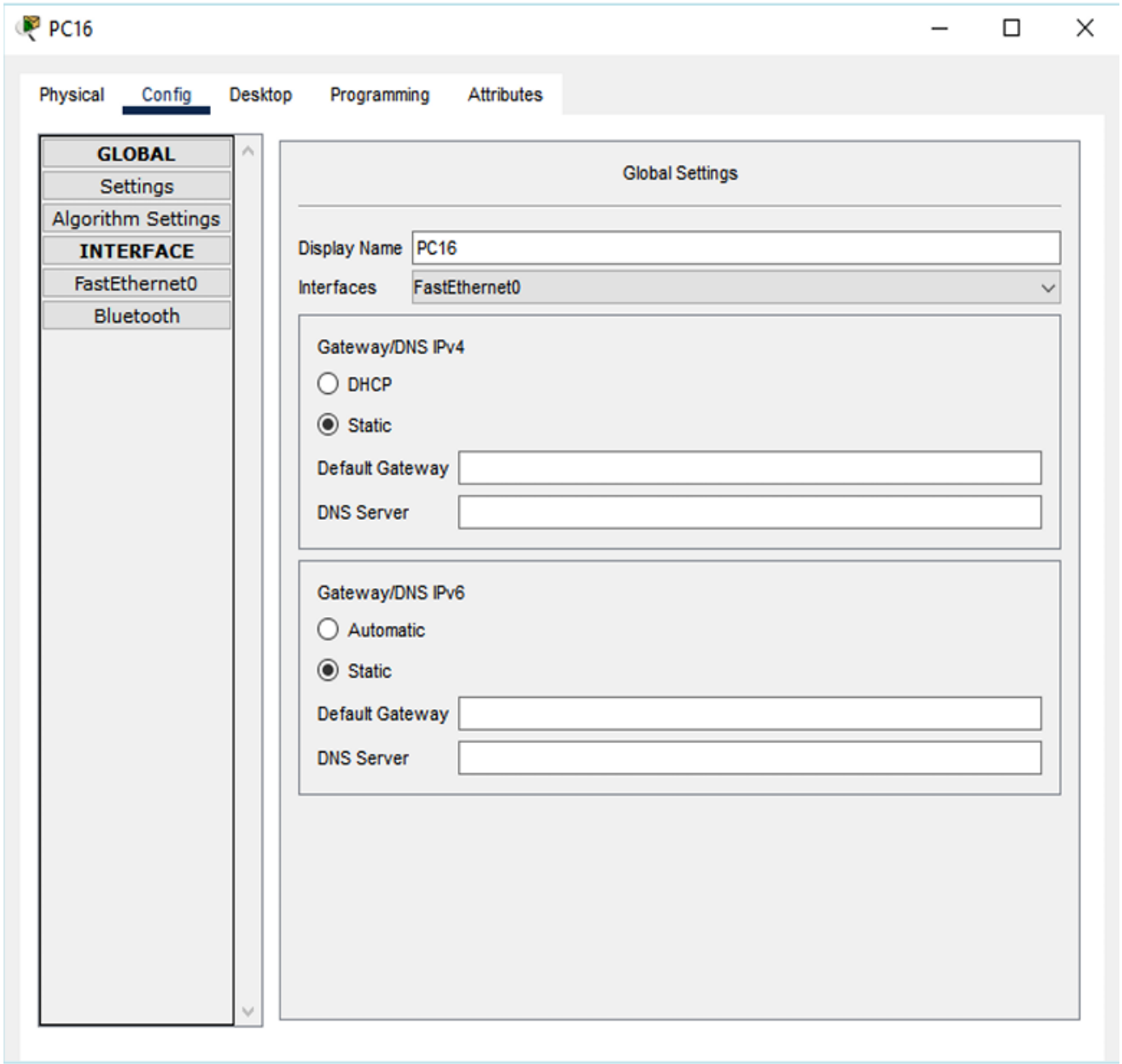

FIGURE 86 – **Fenêtre de configuration d'un PC.**

Pour les switches on utilise l'onglet CLI afin de les configurer avec les commandes nécessaires.

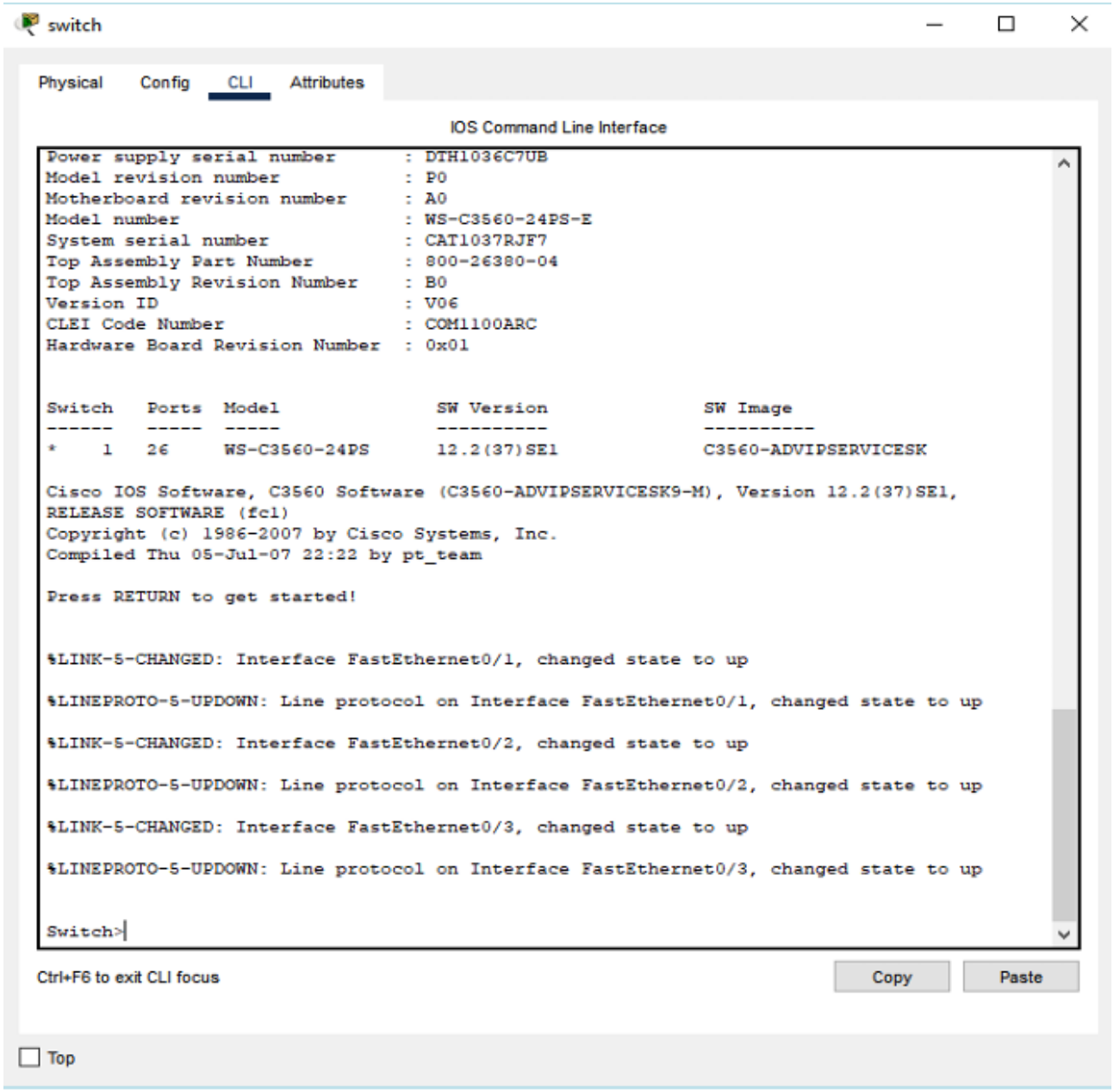

FIGURE 87 – **Fenêtre de configuration d'un PC.**

.6 Mode simulation

Une fois le réseau créé et prêt à fonctionner, il est possible de passer en mode simulation, ce qui permet de visualiser tous les messages échangés dans le réseau. En mode simulation, la fenêtre principale est scindée en deux, la partie de droite permettant de gérer le mode simulation : exécution pas-à-pas, vitesse de simulation, protocoles visibles. La partie gauche de la figure montre la partie simulation et sa partie droite montre les détails obtenus en cliquant sur un message.

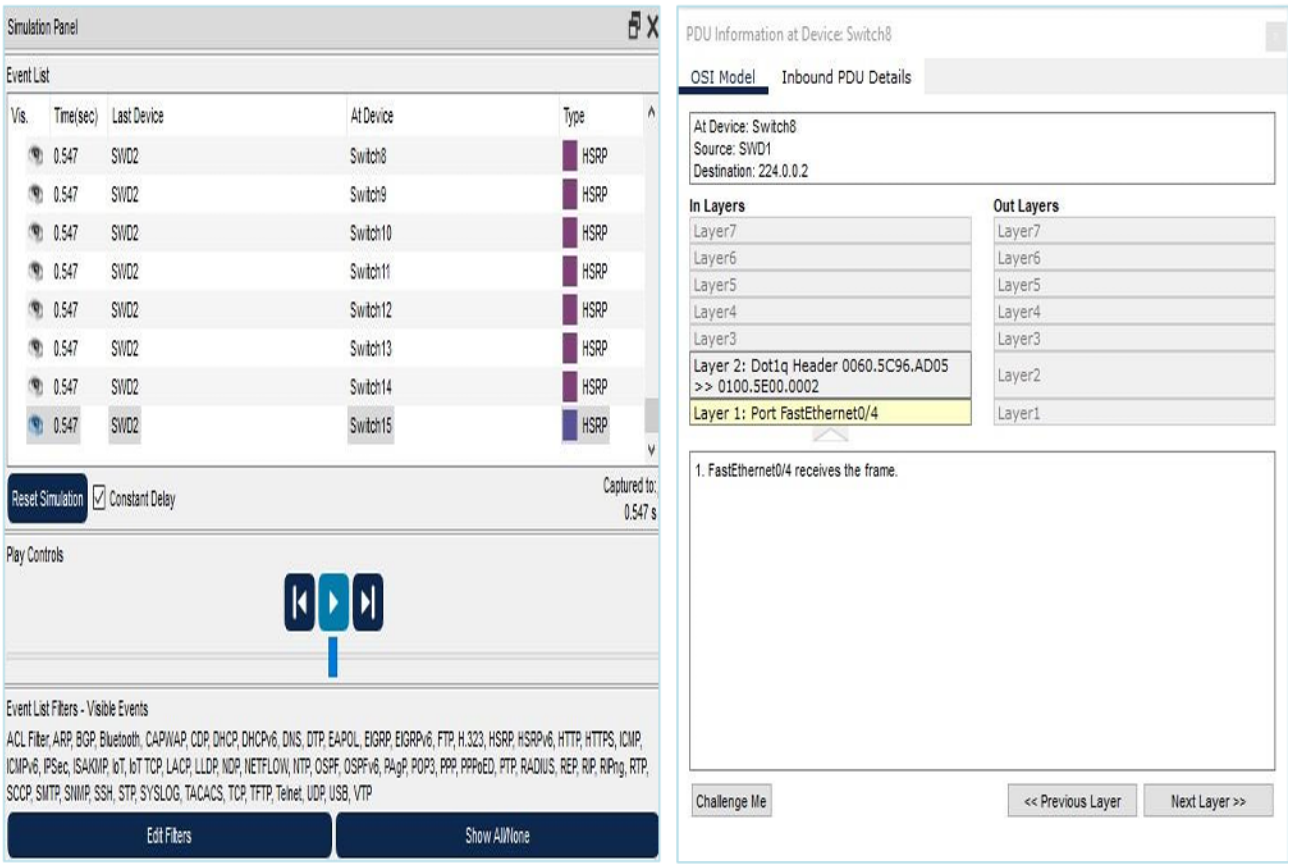

FIGURE 88 – **Fenêtre de configuration d'un PC.**

.7 Invite de commandes

Il est possible d'ouvrir une invite de commandes sur chaque ordinateur du réseau. Elle est accessible depuis le troisième onglet, appelé Desktop, accessible lorsque l'on clique sur un ordinateur pour le configurer (mode sélection). Cet onglet contient un ensemble d'outils dont l'invite de commandes (Command prompt) et un navigateur Internet (Web Browser). L'invite de commandes permet d'exécuter un ensemble de commandes relatives au réseau. La liste est accessible en tapant help. En particulier, les commandes ping, arp, tracert et ipconfig sont accessibles. Si Packet Tracer est en mode simulation, les messages échangés suite à un appel à la commande ping peuvent ainsi être visualisés.

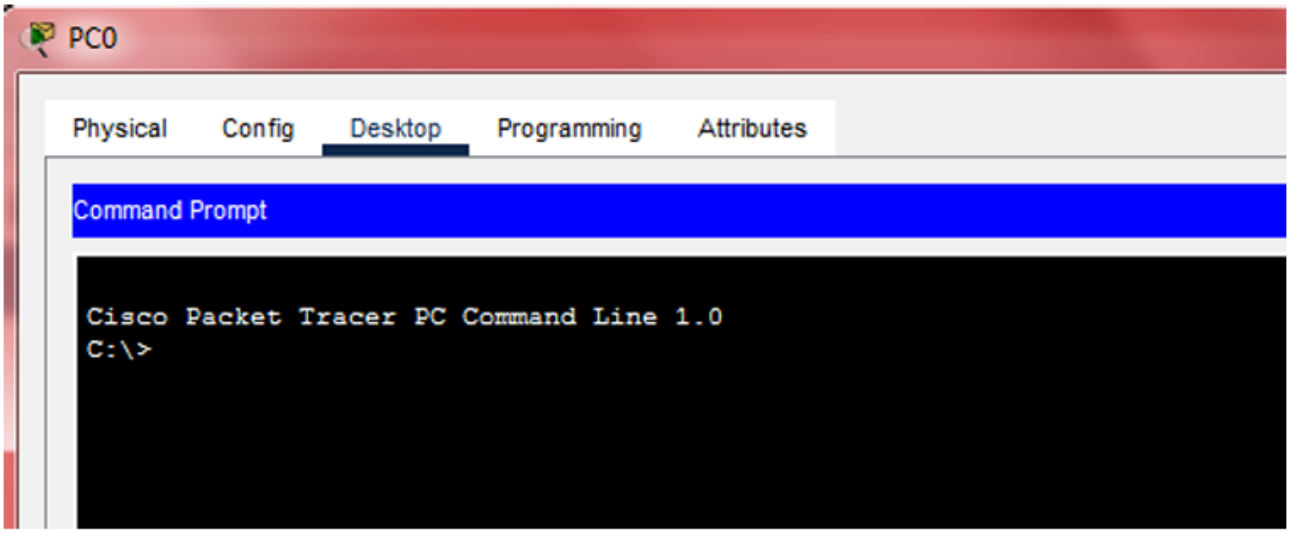

FIGURE 89 – **Commande prompt.**

Bibliographie

[4] Sumit KUMAR, Sumit DALAL et Vivek DIXIT. « The osi model : overview on the seven layers of computer networks ». In : *International Journal of Computer Science and Information Technology Research* 2.3 (2014), p. 461-466.

[5] Philippe ATELIN et José DORDOIGNE. *TCP/IP et les protocoles Internet*. Editions ENI, 2006.

[6] Philippe ATELIN. *Réseaux informatiques-Notions fondamentales (Normes, Architecture, Modele OSI, TCP/IP, Ethernet, Wi-Fi,...)* Editions ENI, 2009.

[7] François LAISSUS. *Cours d'introductiona TCP/IP*. 2009.

[8] WIKIPÉDIA. *Comparaison des modèles OSI et TCP/IP*. Consulté le 31 mai 2025. 2023.

[11] Guillaume CARNINO et Clément MARQUET. « Du mythe de l'automatisation au savoir-faire des petites mains : une histoire des datacenters par la panne ». In : *Artefact. Techniques, histoire et sciences humaines* 11 (2019), p. 163-190.

[18] Mingui ZHANG, Huafeng WEN et Jie HU. *Spanning tree protocol (STP) application of the inter-chassis communication protocol (ICCP)*. Rapp. tech. 2016.

[19] T LI et al. *RFC2281 : Cisco Hot Standby Router Protocol (HSRP)*. 1998.

[20] S NADAS. *Rfc 5798 : Virtual router redundancy protocol (vrrp) version 3 for ipv4 and ipv6*. 2010.

[31] Sébastien LATOUR. *Le Spanning Tree*. `https://slideplayer.fr/slide/2904857/10/images/7/Principe+de+fonctionnement+du+STP.jpg`. Consulté le 25 mai 2025. 2014.

[32] D LEVI et D HARRINGTON. *Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol*. Rapp. tech. 2005.

[33] Jessy Rouyer. *The Multiple Spanning Tree Protocol (MSTP)*. Rapp. tech. qrev-rouyer-mstp-0105. Accessed : 2025-05-18. IEEE 802.1 Working Group, jan. 2005.

[34] Huawei Technologies Co., Ltd. *Understanding STP/RSTP/MSTP*. Rapp. tech. EDOC1100306151. Consulté le 18 mai 2025. Huawei Technologies Co., Ltd., juin 2024.

[35] R Krishnan et al. *Mechanisms for optimizing link aggregation group (LAG) and equal-cost multipath (ECMP) component link utilization in networks*. Rapp. tech. 2015.

[36] Ramki Krishnan et al. *Mechanisms for Optimizing Link Aggregation Group (LAG) and Equal-Cost Multipath (ECMP) Component Link Utilization in Networks*. RFC 7424. Consulté le 13 mai 2025. 2015.

[37] Fakultas Teknologi Informasi dan Komunikasi, Universitas Pasar Sawo Manila. « Load balancing performance in EtherChannel technology using the VLAN Trunking Protocol (VTP) method ». In : *Jurnal Mantik* 3.4 (2020), p. 540-547.

[38] CCNA Philippines. *Diagramme EtherChannel*. `https://www.ccnaphilippines.com/wp-content/uploads/2020/07/UNADJUSTEDNONRAW_thumb_34d.jpg`. Image consultée le 24 mai 2025 via Bing Images. 2020.

[39] El Hassan El AMRI. *Cours EtherChannel*. `https://fr.slideshare.net/ELAMRIELHASSAN/cours-etherchannel`. Consulté le 24 mai 2025. s.d.

[40] Yakov Rekhter, Tony Li et Susan Hares. *RFC 4271 : A border gateway protocol 4 (BGP-4)*. 2006.

[41] FS.com. *Qu'est-ce que BGP et comment fonctionne-t-il ?* Consulté le 29 mai 2025. 2024.

[42] Jessica H. Fong et al. « Better Alternatives to OSPF Routing ». In : *Algorithmica* 43.1–2 (2005).

[44] François Schweizer et al. « The Second Nucleus of NGC 7727 : Direct Evidence for the Formation and Evolution of an Ultracompact Dwarf Galaxy ». In : *The Astrophysical Journal* 853.1 (2018), p. 54.

[45] Shanthi Vineela. *What is Border Gateway Protocol (BGP) ?* Consulté le 13 mai 2025. 2024.

Webographie

[1] Weodeo. *Réseau informatique : comment ça marche ?* Consulté le 27 mai 2025. 2023.
https://www.weodeo.com/digitalisation/reseau-informatique-comment-ca-marche (Consulté le 27 mai 2025).

[2] Techno-Science.net. *Réseau informatique : définition et explications.* Consulté le 27 mai 2025. 2025.
https://www.techno-science.net/definition/3799.html (Consulté le 27 mai 2025).

[3] Wikipédia. *Modèle OSI.* Consulté le 27 mai 2025. 2025.
https://fr.wikipedia.org/wiki/Mod%C3%A8le_OSI (Consulté le 27 mai 2025).

[9] BlueFinch-ESBD. *Qu'est-ce que la haute disponibilité et quel est son objectif ?* Consulté le 30 mai 2025. Juin 2023.
https://bluefinch-esbd.com/fr/quest-ce-que-la-haute-disponibilite-et-quel-est-son-objectif/ (Consulté le 30 mai 2025).

[10] Syloé. *Haute disponibilité informatique.* Consulté le 30 mai 2025. 2024.
https://www.syloe.com/glossaire/haute-disponibilite/ (Consulté le 30 mai 2025).

[12] BaieBrassage. *Onduleur UPS : Définition, rôle, guide de choix.* Consulté le 1 juin 2025. 2024.
https://www.baiebrassage.fr/blog/onduleur-ups-definition-role-guide-de-choix.html (Consulté le 1 juin 2025).

[13] Schneider Electric. *La séparation électrique des circuits.* Consulté le 1 juin 2025. 2025.
https://fr.electrical-installation.org/frwiki/La_s%C3%A9paration_%C3%A9lectrique_des_circuits (Consulté le 1 juin 2025).

[14] TP-Link France. *L'importance de la redondance réseau.* Consulté sur TP-Link France. Juin 2023.
https://www.tp-link.com/fr/blog/1443/l-importance-de-la-redondance-r%C3%A9seau/ (Consulté le 18 mai 2025).

[15] Your IT Department. *What is Redundancy ?* Consulté le 1 juin 2025. 2021.
https://www.your-itdepartment.co.uk/what-is-redundancy/ (Consulté le 1 juin 2025).

[16] Kevin Dooley. *What is Network Redundancy & Why is It Important ?* Consulté le 1 juin 2025. 2024.
https://www.auvik.com/franklyit/blog/simple-network-redundancy/ (Consulté le 1 juin 2025).

[17] François Goffinet. *Cisco EtherChannel : configuration, vérification et dépannage.* Consulté le 1 juin 2025. 2020.
https://cisco.goffinet.org/ccna/redondance-de-liens/cisco-etherchannel-configuration-verification-depannage/ (Consulté le 1 juin 2025).

[21] K TnS. *Automatisation des réseaux avec Ansible et Python : un guide pratique.* Consulté le 1 juin 2025. 2024.
https://www.k-tns.com/automatisation-des-reseaux-avec-ansible-et-python-un-guide-pratique/ (Consulté le 1 juin 2025).

[22] Vaadata. *Audit de sécurité : objectifs, types d'audits et méthodologies.* Consulté le 1 juin 2025. 2024.
https://www.vaadata.com/blog/fr/audit-de-securite-objectifs-types-daudits-et-methodologies/ (Consulté le 1 juin 2025).

[23] Yann Fralo. *Équilibrage des charges : l'incontournable d'une infrastructure haute disponibilité.* Consulté le 1 juin 2025. 2020.
https://www.silicon.fr/Thematique/cloud-1370/Breves/Equilibrage-charges-incontournable-infrastructure-haute-disponibilite-458902.htm (Consulté le 1 juin 2025).

[24] Capterra. *Redondance de réseau.* Consulté sur Capterra. 2025.
https://www.capterra.fr/glossary/628/network-redundancy (Consulté le 18 mai 2025).

[25] TP-Link. *L'importance de la redondance réseau.* Consulté le 18 mai 2025. TP-Link. 2023.
https://www.tp-link.com/fr/blog/1443/l-importance-de-la-redondance-r%C3%A9seau/.

[26] abcXperts. *HSRP, VRRP, GLBP : Entendiendo los protocolos clave para la redundancia en redes*. Consulté le 27 mai 2025. 2024.
https://abcxperts.com/fr/hsrp-vrrp-glbp-entendiendo-los-protocolos-clave-para-la-redundancia-en-redes/.

[27] Julien Lavergne. *Mise en place du protocole HSRP | Cisco*. IT-Connect. 2014.
https://www.it-connect.fr/mise-en-place-du-protocole-hsrp/ (Consulté le 18 mai 2025).

[28] Valentin Weber. *HSRP*. Consulté le 27 mai 2025. 2014.
https://www.networklab.fr/hsrp/.

[29] Cyberopti. *Protocole GLBP : Exemples et Configuration*. Consulté sur Cyberopti. Oct. 2024.
https://cyberopti.com/protocole-glbp-exemples-et-configuration/ (Consulté le 18 mai 2025).

[30] abcXperts. *HSRP, VRRP, GLBP : Comprendre les protocoles clés pour la redondance réseau*. Consulté le 18 mai 2025. 2025.
https://abcxperts.com/fr/hsrp-vrrp-glbp-entendiendo-los-protocolos-clave-para-la-redundancia-en-redes/.

[43] Cisco Tracer. *HSRP (Hot Standby Routing Protocol)*. Consulté le 13 mai 2025. 2014.
https://ciscotracer.wordpress.com/2014/03/13/hsrp-hot-standby-routing-protocol/ (Consulté le 13 mai 2025).

[46] NetworkLab. *VRRP : Virtual Router Redundancy Protocol*. Consulté le 27 mai 2025. 2024.
https://www.networklab.fr/vrrp/.

[47] Wikibooks contributors. *Les réseaux informatiques/Les modèles OSI et TCP*. Wikibooks, le livre libre. 2024.
https://fr.wikibooks.org/wiki/Les_r%C3%A9seaux_informatiques/Les_mod%C3%A8les_OSI_et_TCP (Consulté le 30 mai 2025).

[48] FC MICRO. *Panne informatique : causes et conséquences pour les entreprises*. Consulté le 31 mai 2025. 2022.
https://fcmicro.net/panne-informatique-causes-et-consequences/.

[49] Michael Ponomarenko. *L'importance de la redondance réseau*. Consulté le 1 juin 2025. 2023.
https://www.tp-link.com/fr/blog/1443/l-importance-de-la-redondance-r%C3%A9seau/ (Consulté le 1 juin 2025).

Résumé

Aujourd'hui, la haute disponibilité est devenue indispensable au bon fonctionnement des réseaux informatiques. Dans ce contexte, cette étude propose une solution de haute disponibilité et de répartition de charge pour le réseau LAN/WAN du site Cevital-Béjaïa, en s'appuyant sur des protocoles tels que VTP, STP, HSRP et OSPF. Cette solution vise à intégrer une redondance au niveau des liens et des équipements du réseau. À l'aide du simulateur Packet Tracer, une architecture hiérarchique interconnectant différents VLANs est mise en place, afin de garantir la disponibilité du réseau et d'assurer une communication fluide entre les postes de travail.

Mots clés : Réseau LAN/WAN , La haute disponibilité, Cevital , Vlan's , HSRP.

Abstract

Nowadays, high availability has become essential to ensure the proper functioning of computer networks. In this context, this study proposes a high availability and load balancing solution for the LAN/WAN network of the Cevital-Béjaïa site, based on the HSRP protocol. The goal of this solution is to implement redundancy at the level of both network links and devices. Using the Packet Tracer simulator, a hierarchical architecture interconnecting different VLANs is designed to ensure network availability and enable smooth communication between workstations.

Keywords : LAN/WAN network, High availability , Cevital , VLAN's,HSRP.